Protecting Critical Infrastructure
Series Editors: Simon Hakim · Erwin A. Blackstone · Robert M. Clark

Robert M. Clark
Simon Hakim *Editors*

Cyber-Physical Security

Protecting Critical Infrastructure at the State and Local Level

Springer

Protecting Critical Infrastructure

Volume 3

Series editors

Simon Hakim, Philadelphia, PA, USA
Erwin A. Blackstone, Philadelphia, PA, USA
Robert M. Clark, Cincinnati, OH, USA

More information about this series at http://www.springer.com/series/8764

Robert M. Clark · Simon Hakim
Editors

Cyber-Physical Security

Protecting Critical Infrastructure at the State and Local Level

Springer

Editors
Robert M. Clark
Cincinnati, OH
USA

Simon Hakim
Department of Economics
Temple University
Philadelphia, PA
USA

Protecting Critical Infrastructure
ISBN 978-3-319-32822-5 ISBN 978-3-319-32824-9 (eBook)
DOI 10.1007/978-3-319-32824-9

Library of Congress Control Number: 2016938414

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG Switzerland

Cybersecurity challenges have become one of the defining issues of our time. These challenges include denial of service, theft and/or manipulation of data. Damage to critical infrastructure through cyber-based attacks will have a significant impact on national security, the economy, and the livelihood and safety of governments and individual citizens throughout the world. We, therefore, dedicate this book to the men and women, including the authors of the manuscripts in this volume, who have devoted their lives and careers to protecting society against these cyber threats. We would like to extend a special acknowledgment to the men and women of the US Government Accountability Office (US GAO), who provide an enormous service to the citizens of the United States and the world through their objective and insightful studies. We have utilized many of their cyber-security studies as background for this book.

Robert M. Clark
Simon Hakim

Contents

Contributors

Dr. Mamoun Alazab is a Lecturer of Cybersecurity at the Department of Policing, Intelligence and Counter Terrorism, Macquarie University. Dr. Alazab holds a Ph.D. in IT Cyber Security from the Federation University of Australia. In early 2012, he began a 3 year appointment at the Australian National University (ANU) as a Research Fellow where he co-founded the ANU Cybercrime Observatory with Prof. Broadhurst. Dr. Alazab has previously worked overseas, which included working for a year as an Assistant Professor at the American University of Middle East in Kuwait. Dr. Alazab was also awarded Japan's most prestigious academic award, a 2-year postdoctoral fellowship from the Japan Society for the Promotion of Science (JSPS) through the Australian Academy of Science (July–September 2015). Dr. Alazab has published more than 50 research peer-reviewed papers, and is widely cited. He is a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE). He has worked closely with government and industry on many projects, including International Business Machines Corporation (IBM), the Australian Federal Police (AFP), the Australian Communications and Media Authority, Westpac, and the Attorney General's Department. Dr. Alazab's research is multi-disciplinary and includes both technological and criminological perspectives of computer crime, with a focus on crime detection and prevention. His general research focus is on the role of the Internet in facilitating crime.

Richard D. Alexander is a network architecture and security consultant for Internet Service Providers (ISPs) and provides consulting support to a wide range of rural and metropolitan ISPs in North America, Europe, and Africa. Mr. Alexander has worked with a wide variety of traditional supervisory control and data acquisition systems/distributed control systems (SCADA/DCS) systems. He has designed and implemented secure interconnections for SCADA/DCS systems over machine-to-machine (M2M), cellular and public Internet paths. Previously, Mr. Alexander has supported advanced instrumentation systems used for event detection purposes in the water and wastewater sectors including instrumentation used in water security initiatives led by the United States Environmental Protection Agencies (EPA's) National Homeland Security Research Center. Mr. Alexander

holds a B.A. (Honors First Class) degree and a postgraduate Diploma in Computing focused on Information Security and Networking from the Open University (UK) and has served as an instructor on a wide range of modules for cybersecurity degrees.

S. (Sanne) Boes M.Sc. studied criminology at the University of Leiden (the Netherlands). Since 2012, she has worked at the Cybersafety Research Group of the Netherlands (NHL) University of Applied Sciences and the Police Academy. In this position, she is a Ph.D. student affiliated to the Open University of the Netherlands. Her Ph.D. study is about the fight against online banking fraud, with special attention to public–private partnerships between criminal justice authorities and the banking sector. The aim of her study is to outline the legal framework of cooperation between public and private actors for criminal justice purposes and to make a proposal to improve it. Resultantly, information gathered by means of private investigation could be used in criminal proceedings in a legally acceptable way. Her research is part of the Dutch Research Program on Safety and Security of Online Banking. This program is funded by the Dutch banking sector, represented by the Dutch Banking Association (NVB), the Police Academy, and the Cybercrime Program of the Dutch police.

Prof. Roderic Broadhurst is a Professor of Criminology, Research School of Social Sciences, Australian National University (ANU) and previously the Deputy Director of the Australian Research Council Centre of Excellence in Policing and Security, ANU. He is a graduate of the University of Western Australia and Cambridge, Associate Fellow of the Australian Institute of Criminology, Hon. Professor at Griffith University (2008–2010) and the University of Hong Kong (2005–2009). He was formerly Senior Fellow, Crime Research Centre University of Western Australia (1989–1994); Associate Professor, the University of Hong Kong (1994–2005); Chair of the Hong Kong Criminology Society (2003–2006), and Head of the School of Justice (Queensland University of Technology 2005–2008). He was also founding fellow of the Hong Kong Centre for Criminology (1998), associate editor of the Australian and New Zealand (ANZ) Journal of Criminology (1999–2004; editorial board 2012–) and foundation editor of the *Asian Journal of Criminology* (2005). His 40-year career as a practitioner and researcher has included work in prisons, remote area public health, post-conflict Cambodia, and homicide investigation. He is an expert on the measurement of recidivism and has published on this topic in the British J. Criminology, J. Quantitative Criminology, and the J. Crime Research Delinquency and the ANZ J. Criminology. He has led research on crime victims in Cambodia and China and currently directs the ANU Cybercrime Observatory. Recent books include Business and the Risk of Crime in China (ANU Press 2011), Policing in Context (Oxford 2009), and Violence and the Civilizing Process in Cambodia, (Cambridge 2015). Three recent articles have been translated into Chinese and another into Vietnamese. His current research includes crime and modernization, homicide, comparative studies of crime, recidivism, organized crime in China and Asia, and crime in cyberspace.

Dr. Robert M. Clark is an independent consultant in environmental engineering and public health. As a consultant, Dr. Clark has worked on homeland security issues with Sandia National Laboratories, the US Environmental Protection Agency (USEPA) and Rutgers University (Newark Campus), among others. He served as an environmental engineer in the U.S. Public Health Service and the U.S. EPA from 1961 to August 2002 and was Director of the USEPA's Water Supply and Water Resources Division (WSWRD) for 14 years (1985–1999). In 1999 he was appointed to a Senior Expert Position in the USEPA with the title Senior Research Engineering Advisor and retired from the USEPA in August of 2002. Dr. Clark was a member of USEPA's Water Protection Task Force and was USEPA's liaison for homeland security research. Dr. Clark has published over 400 papers and 6 books and has been professionally active in several organizations where he served in numerous leadership positions. He is a lifetime member of both the American Water Works Association (AWWA) and the American Society of Civil Engineers (ASCE). Dr. Clark is recognized both nationally and internationally and has received numerous awards for his work. He was a member of the National Research Council's Committee on "Public Water Distribution Systems: Assessing and Reducing Risks." Clark holds B.S. degrees in Civil Engineering from Oregon State University (1960) and in Mathematics from Portland State University (1961), M.S. degrees in Mathematics from Xavier University (1964), and Civil Engineering from Cornell University (1968) and a Ph.D. in Environmental Engineering from the University of Cincinnati (1976). He is a registered engineer in the State of Ohio.

Andrew F. Ginter is the VP Industrial Security at Waterfall Security Solutions. Andrew spent 25 years leading the development of data communications, industrial control systems, information technology/operational technology (IT/OT) middleware, and industrial cybersecurity products for Develcon, Hewlett-Packard, Agilent Technologies and Industrial Defender, and holds a number of patents for IT/OT middleware and industrial cybersecurity technologies. At Waterfall, Andrew leads the industrial cybersecurity team, writes and speaks frequently on industrial cybersecurity topics, and represents Waterfall to standards bodies. He is the co-chair of the international standards association (ISA) SP-99 TG1 WG1 group, and contributes regularly to the National Institute of Standards and Technology (NIST), North American Electric Reliability Corporation Critical Infrastructure Program (NERC CIP), National Cybersecurity Center of Excellence (NCCoE), Industrial Internet Consortium (IIC), ISA SP-99, and other industrial cybersecurity standards. Andrew holds a B.Sc. in Applied Mathematics and an M.Sc. in Computer Science, both from the University of Calgary.

Dr. Simon Hakim is Professor of Economics and Director of the Center for Competitive Government at Temple University. He is currently editing a book series on Protecting Critical Infrastructures with Springer Publisher. He earned M.A. and Ph.D. degrees in Regional Science from the University of Pennsylvania. He also holds an M.Sc. degree in City and Regional Planning from the Technion, Israel Institute of Technology, and a B.A. in Economics at Hebrew University in

Jerusalem. His special areas of research and teaching include privatization, public policy, private/public police, and homeland security. Dr. Hakim has published 58 scientific articles in leading economic, criminal justice, security, and public policy journals. He has written over 60 professional articles, and written and edited 17 books. He collaborated with Prof. Blackstone on a major textbook dealing with the security industry. Dr. Hakim has conducted several funded research and consulting projects for the U.S. Departments of Justice and Labor, the Commonwealth Foundation, the Independent Institute, the Alarm Industry Research and Education Foundation, the City of Philadelphia, the Philadelphia International Airport, ADT, Vector Security, the private prison industry, and other leading security companies. See, http://www.fox.temple.edu/ccg

Dr. Jiow Hee Jhee is a Lecturer at the Singapore Institute of Technology (SIT). Prior to joining SIT, Dr. Jiow was a Visiting Fellow with the Asia Research Centre, Murdoch University, under the auspices of the Australian Endeavour Award, where he studied the regulation of cybercrime. He has also served as Associate Lecturer at the Singapore Institute of Management, teaching media law and ethics. Recipient of the National University of Singapore's Graduates Students Teaching Award, he has taught undergraduates on cybercrime, surveillance, media governance, media literacy, advertising strategies, social research methods, and social policy. Dr. Jiow's research interests include video gaming, cybercrime, media's impact on the domestic realm and parents' response to media influence on their children. He has published in journals such as *International Journal of Cyber Criminology*, *First Monday*, and *Bulletin of Science, Technology and Society*. Dr. Jiow speaks publicly on various parenting issues, and has trained more than 40,000 local and international youths, and 4,000 parents on media literacy, life skills, healthy relationships, and communication. Being a pioneer of the cyber wellness movement in Singapore, he was involved in setting up the first Cyber Wellness Centre in Singapore in 2006.

E. R. (Rutger) Leukfeldt studied criminology at the University of Leicester (M.Sc. with merit). Currently, he is researcher of cybercrime at the Cyber Safety Research Group of NHL University of Applied Sciences and the Dutch Police Academy. He is also Ph.D. candidate of Organized Cybercrime at the Open University of the Netherlands. His current research (2012–2016) aims to provide insight into criminal networks that are specialized in financial cybercrimes such as credit card fraud and phishing. This research is part of the Dutch Research Program on Safety and Security of Online Banking. This program is funded by the Dutch banking sector, represented by the Dutch Banking Association (NVB), the Police Academy and the Cybercrime Program of the Dutch police. In the period 2007–2013, Rutger carried out several studies on the nature and the extent of cybercrime and on the organization of law enforcement in relation to cybercrime. He has published in various (international) peer-reviewed journals on this topic.

Trent D. Nelson is currently a Cybersecurity Consultant for Critical Infrastructure, and works directly with asset owner for 12 years to identify cybersecurity weakness, and develops mitigation techniques to defend against cyber attacks. Trent has been Supervisor for the Cyber Security Research Departments Advanced Cyber Defense Center at Idaho National Laboratory and Principal Engineer/Scientist with a Bachelor's degree in Computer Information Systems (CIS). He has been working with Industrial Control Systems (ICS), IT Systems, and CIS systems for 25 years. Trent was also the Cyber Security Assessment Lead for 10 years with the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) for the DHS National Cyber Security Division. His responsibilities include cyber tools, testing, and evaluation of critical infrastructure. Trent's oversight of assessment activities has required the development of test plans, vulnerability assessments, and information gathering efforts to identify threat vectors, and mitigations to unsecured systems. He was also the Deputy Director for the Operations Center for 5 years at the INL.

Dr. Dennis Kengo Oka works as a senior consultant at ETAS K.K. Embedded Security (ESCRYPT), Japan. He has been involved in vehicle security research since 2006. Dennis received his Ph.D. in Computer Security from Chalmers University of Technology in Sweden in 2009. In the past, he has worked with Volvo Car Corporation in Sweden where he researched authentication and integrity principles for wireless communication with vehicles. Dennis has also conducted research at Stanford Research Institute (SRI) International in California, USA in the areas of security in wireless sensor networks and Bluetooth communication. Moreover, Dennis has conducted research at Waseda University in Japan in the areas of security and dependability in embedded systems. He was also involved in a research study with the European Network and Information Security Agency (ENISA) regarding Internet of Things (IoT) security for an air travel scenario. Dennis also worked for Swedish Institute of Computer Science (SICS) where he researched security approaches using virtualization on multi-core embedded devices. Prior to joining ETAS, he worked for Bosch Automotive Service Solutions K.K. in Japan where his focus was on solutions for diagnostics and engine control unit (ECU) reprogramming. Dennis has over 30 publications at international conferences and several journals, magazine and book publications. His research interests include vehicle security, wireless security, embedded security and intrusion detection. e-mail: dennis-kengo.oka@etas.com

Srinivas Panguluri is Senior Engineer who works for CB&I Federal Services LLC in the Cincinnati Office. He has over 25 years of hands-on technical and management experience in conducting a variety of applied research. He has conducted research on behalf of the U.S. Environmental Protection Agency's (EPAs) Office of Research and Development (ORD) in Cincinnati and other field locations. Mr. Panguluri has implemented a variety of EPA National Homeland Security Research Center's (NHSRCs) water security related initiatives since the inception of NHSRC. Mr. Panguluri has designed, implemented, and maintained

Supervisory Control and Data Acquisition (SCADA) systems and associated Information Technology (IT) components including computer networks, databases, and websites for online monitoring and process control. Mr. Panguluri has served as a co-author and lead author for multiple EPA-published reference guides in the water sector. He has also co-authored book chapters and journal/conference publications on cybersecurity. Mr. Panguluri holds a B.S. in Engineering from Sri Venkateswara University, India (1990) and an M.S. in Engineering from the University of Toledo (1993). At Toledo, he was the recipient of the Outstanding Master's Research Award from the Sigma Xi Scientific Research Society. In addition, Mr. Panguluri possesses several information technology (IT) certifications including Microsoft Certified Systems Engineer (MCSE), A+, SQL database administration, SAIR Linux, etc. He is also a registered Professional Engineer in the State of Ohio and can be reached via email at Srinivas. e-mail: Panguluri@CBIFederalServices.com

Dr. Jyri K. Rajamäki is currently a Principal Lecturer in Information Technology at Laurea University of Applied Sciences (UAS), Finland. He is Adjunct Professor of Critical Infrastructure Protection and Cyber Security at the University of Jyväskylä. Dr. Rajamäki worked 10 years (1986–1996) for Telecom Finland, with his main tasks being uninterruptible power supplies, electromagnetic compatibility (EMC), and electromagnetic pulse protection. From 1996 to 2006, Dr. Rajamäki acted as Senior/Chief Engineer for Safety Technology Authority of Finland where his main assignment was to make the Finnish market ready for the European Electromagnetic Compatibility (EMC) Directive. For 17 years, Dr. Rajamäki was the secretary or a member of Finnish national standardization committee on EMC, and he represented 15 years Finland at International Electrotechnology Commission (IEC), Comité International Spécial des Perturbations Radioélectriques (CISPR), Comité Européen de Normalisation Électrotechnique (CENELEC), and European Telecommunications Standards Institute ETSI EMC meetings. He was the Chairman of Finnish Advisory Committee on EMC from 1996 to 2006. Since 2006, Dr. Rajamäki has been the head of Data Networks Lab of Laurea UAS. Dr. Rajamäki has been the scientist in charge, national coordinator, and scientific supervisor for several national and European research projects. For the European Research Area he has acted as the evaluator of the projects. He is currently an advisor board member of the HARMONISE (A Holistic Approach to Resilience and Systematic Actions to Make Large Scale Built Infrastructure Secure) FP7 Project. His current research interests are resilient cyber-physical systems, and overall governance (generation, transmission, storage, processing, sharing, collective use, deletion) of safety critical and/or classified information. Dr. Rajamäki has authored more than 150 scientific publications. Dr. Rajamäki holds M.Sc. degree (1991) in Electrical Engineering from Helsinki University of Technology, Lic.Sc. (2000), and D.Sc. (2002) degrees in Electrical and Communications Engineering from Helsinki University of Technology, and a Ph.D. degree (2014) in Mathematical Information Technology from University of Jyväskylä.

Ms. Natalie Sjelin is the Associate Director of Training at the Center for Infrastructure Assurance and Security (CIAS) at the University of Texas at San Antonio (USTA). For the past 14 years, Ms. Sjelin has played a key role in training and exercise initiatives assisting communities across the nation to develop viable and sustainable Community Cyber Security Programs for their jurisdictions. Ms. Sjelin managed, coordinated, and facilitated Community Cyber Security exercises and leads the training team in building robust training capabilities and delivering information security training, workshops, seminars, and conferences aimed at a national audience for the Department of Homeland Security, military and industry partners. Ms. Sjelin has been very active in presenting cybersecurity topics throughout the nation and US Territories to professional associations, community leadership, and at national conferences. She has co-authored several articles on community cybersecurity and most recently a book chapter on the Community Cyber Security Maturity Model (CCSMM) which serves as a framework for states and communities to develop community cybersecurity programs. In addition to being the Associate Director of Training for the CIAS at UTSA, Ms. Sjelin is also the Director for the Information Sharing and Analysis Organizations (ISAO) Standards Organization (SO) support. In this role she is working with newly formed ISAOs which desire to participate in the nation's cybersecurity information sharing efforts.

Dr. Howard A. Stern is Associate Professor of Management and Co-Director of the MBA Program at Carlow University in Pittsburgh, Pennsylvania. He also serves as Special Assistant to the Provost for academic initiatives, including online programming and the development of university collaborations and partnerships. Upon election by his faculty colleagues, Stern serves as the faculty representative to the University's Board of Trustees. Stern has published in the Journal of Information Technology Management and the Journal of Information Technology Teaching Cases and has presented at numerous national and international conferences. His primary research interests include the relationship between politics and technology, e-government innovations, e-discovery, and social media. In 2015, Stern received the Sisters of Mercy Award for Excellence in Advising. Before joining Carlow, Stern served as the Chief Information Officer for the City of Pittsburgh from 2004 to 2012, where he was responsible for citywide technology projects such as the installation of surveillance cameras and the design and implementation of financial, Enterprise Resource Planning (ERP), and public safety systems. In 2011, he was named CIO of the Year by the Pittsburgh Technology Council.

Lior Tabansky is a scholar of cyber power at Tel Aviv University's Blavatnik Interdisciplinary Cyber Research Center (TAU ICRC). Mr. Tabansky's doctoral thesis in Political Science develops comparative international cybersecurity analysis with Military Innovation framework. Lior's strategic cybersecurity expertise stems from a unique combination: the service in the Israeli Air Force, subsequent career designing and managing business Information and Communications Technology

(ICT) infrastructure, postgraduate political science education, and a proven commitment to interdisciplinary academic policy-oriented research. Mr. Tabansky wrote and published the Israeli inaugural cybersecurity scholarship while at the Institute for National Security Studies (INSS) think-tank in Tel Aviv. Mr. Tabansky's recent book *Cybersecurity in Israel*, co-authored with Prof. Isaac Ben-Israel, provides the first detailed account and strategic analysis of Israeli cyber power. Published by Springer, the comprehensive analysis accentuates the Israeli strategy and the national innovation ecosystem interplay, and includes insights into the Israeli Defense Forces (IDF's) cyber warfare experience.

Andrew E. Tucci a Captain in the United States Coast Guard (USCG), has 25 years of experience, predominantly in maritime security, critical infrastructure protection, cybersecurity, contingency planning, oil spill response. His experience includes interagency policy development experience at national level. His work on preparedness and emergency response includes work with the National Response Team, the National Response Framework, Hurricane Sandy, the Deepwater Horizon oil spill, 9–11, and Western Rivers flooding. He wrote the Coast Guard's policy concerning Place of Safe Refuge planning. He is currently Chief, Office of Facilities Compliance, U.S. Coast Guard Headquarters, Washington DC. In this position he is responsible for policy development and program management for safety, security, and environmental standards for 361 U.S. ports and ~3,000 individual waterfront facilities. He leads the Coast Guard efforts to improve global supply chain security and resilience. His other coast guard assignments include the following:

- July 2008–July 2011: Deputy Sector Commander, Sector Ohio Valley, Louisville KY.
- July 2004–July 2008: Program Manager, Coast Guard Headquarters, Oil and Hazardous Materials Incident Preparedness.
- July 1999–August 2002: Coast Guard Operations, Marine Safety Office Puget Sound, Seattle Washington.
- April 1990–July 1999, various Coast Guard assignments in Alaska and Maine involving port security, commercial vessel and port facility inspections, marine casualty investigation, oil spill response, law enforcement, and search and rescue operations.

Captain Tucci's awards, qualifications, and training include Coast Guard Meritorious Service Medal (2x); Commendation Medal (4x); Type II Incident Commander; Qualified Marine Inspector; Marine Casualty Investigator; Pollution Investigator; Federal On-Scene Coordinator's Representative; and Search and Rescue Supervisor.

His education includes Master of Marine Affairs, University of Washington, Seattle Washington, 2004. He has also earned a certificate in Global Trade, Transportation, and Logistics and a Bachelor of Science, Business Administration, Miami University, Oxford Ohio, 1989.

Dr. Gregory White has been involved in computer and network security since 1986. He spent 30 years with the Air Force and Air Force Reserves. He obtained his Ph.D. in Computer Science from Texas A&M University in 1995 conducting research in the area of computer network intrusion detection and he continues to conduct research in this area today. He currently serves as the Director of the Center for Infrastructure Assurance and Security (CIAS) and is Professor of Computer Science at The University of Texas at San Antonio (UTSA). Dr. White has been involved in security instruction for many years. He taught at the U.S. Air Force Academy for 7 years where he developed and taught courses on computer security and information warfare. He helped build the nation's first undergraduate information warfare laboratory while at the academy. At UTSA Dr. White continues to develop and teach courses on computer and network security. He has also been very active in the development and presentation of cybersecurity exercises for states and communities around the nation and with the development of training designed to help states and communities develop viable and sustainable cybersecurity programs. Additionally he is very active in development of cybersecurity competitions and was instrumental in the development of the National Collegiate Cyber Defense Competition and the CyberPatriot National High School Cyber Defense Competition. Dr. White has written numerous articles and conference papers on computer security. He is also the co-author for five textbooks on security and has written chapters for two others. His current research interests include an examination of organizational issues affecting computer security, secure information sharing, high-speed intrusion detection, infrastructure protection, community cyber incident response, and the development of the Community Cyber Security Maturity Model (CCSMM) which serves as a guide for states and communities desiring to build their own viable and sustainable cybersecurity programs. Dr. White received the 2011 Educator Leadership award for Exceptional Leadership in Information Assurance Education at the Colloquium for Information Systems Security Education (CISSE). In 2012 he was awarded the Air Force Association Distinguished Sustained Aerospace Education Award for his efforts in cybersecurity education. In 2014 he was made a Distinguished Fellow of the Information Systems Security Association. In addition to being the director of the CIAS at UTSA, Dr. White also serves as the Executive Director of the Information Sharing and Analysis Organizations (ISAO) Standards Organization (SO) and is the Director of the National Cybersecurity Preparedness Consortium (NCPC).

Dr. Scott J. White is a Criminologist and Associate Clinical Professor at Drexel University (Philadelphia, PA). He holds a B.A. in Psychology and Political Science from York University (Toronto, Canada), an M.A. in Political Studies with a concentration in terrorism from the University of Guelph (Guelph, Canada), and a Ph.D. in Criminology from the University of Bristol (Bristol, England). Dr. White holds a Queen's Commission and was an Officer with Canadian Forces Intelligence Command. In addition to following his Ph.D. studies, Dr. White was an Intelligence Officer with the Canadian Security Intelligence Service. In 2010, Dr. White joined MONAD Security Audit Systems as Associate Consultant. His areas of interests

include cybercrime, counter-terrorism, and infrastructure protection. Dr. White has consulted with a variety of law enforcement agencies in the United States, the UK, and Canada. Today, Dr. White is Associate Clinical Professor of National Security, a Member of Drexel University's Cybersecurity Institute, and Director of the Computing and Security Technology Program at Drexel University.

Richard P. Wyman BSME, MSME, CISSP Professional Control Systems Engineer, is a subject matter expert in industrial control system cybersecurity for a national laboratory. For the past 7 years he has helped operators of critical infrastructure, especially the water sector, improve the cyber defenses of their control systems through assessments and training. Previous to his career at the laboratory, Richard worked 25 years as a control systems engineer at a petroleum refinery and water utility. As the project manager and technical lead, he completed the installation of a large distributed Supervisory Control and Data Acquisition (SCADA) system for a northern California water utility. This distributed SCADA system supported operations for hydroelectric power generation, water treatment, and water distribution. Richard has also supported offshore oil and gas exploration as a drilling engineer in Australia, Singapore, Malaysia, Canada, and Brazil. He earned a Bachelor's degree from Brigham Young University and a Master's degree from University of Washington in Mechanical Engineering. In addition to his technical expertise, Richard has given presentations on controls and communications at several professional conferences and presented workshops on industrial communications, instrumentation, and control systems in North America and Europe.

Chapter 1
Protecting Critical Infrastructure at the State, Provincial, and Local Level: Issues in Cyber-Physical Security

Robert M. Clark and Simon Hakim

Abstract The issue of cyber-security is currently having and will continue to have a major impact on organized society. Cyber-threats to infrastructure, and other assets, are of growing concern to policymakers throughout the world. For example, the President of the United States (US), in 2009, declared cyber threats to be among "the most serious economic and national security challenges we face as a nation" and stated that "America's economic prosperity in the 21st century will depend on cyber-security." Cyber-attacks might include denial of service, theft or manipulation of data. Information and communications technology (ICT) is becoming ubiquitous and many ICT devices and other components are interdependent. Therefore disruption of one component may have a negative, cascading effect on others. It is clear that cyber-security issues include not only the threats associated with information technology but also involves physical threats to Critical Infrastructure (CI). Damage to critical infrastructure through a cyber-based attack could have a significant impact on security at the national level, the economy, and the livelihood and safety of citizens. It is therefore important that national governments develop comprehensive strategies to deal with issues related to cyber-security. As critical infrastructure becomes more dependent on computer technology and increasingly tied to the internet, cyber-attacks against communication networks and system are growing in number and are becoming more sophisticated. Several examples are presented, that illustrate the impact of cyber-attacks on international security as well as attacks on critical infrastructure. In addition, a number of approaches that might help deal with cyber-security are suggested including the development of public-private partnerships.

R.M. Clark (✉)
Environmental Engineering and Pubic Health Consultant, 9627 Lansford Drive, Cincinnati, OH 45242, USA
e-mail: rmclark@fuse.net

S. Hakim
Center for Competitive Government at the Fox School, Temple University, Philadelphia, PA 19122, USA
e-mail: simon.hakim@temple.edu

R.M. Clark and S. Hakim (eds.), *Cyber-Physical Security*,
Protecting Critical Infrastructure 3, DOI 10.1007/978-3-319-32824-9_1

Acronyms

APT	Advanced persistent threats
ATM	Automated teller machine
CCSMM	Community cyber security maturity model
CI	Critical infrastructure
CIO	Chief information officer
CIP	Critical infrastructure protection
CMU	Carnegie Mellon University
CP	Cyber-physical
DHS	Department of Homeland Security
DOD	Department of Defense
DSL	Digital subscriber line
ECA	Electronic control units
EPA	Environmental Protection Agency
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FIMSA	Federal Information Security Act
GAO	Government Accountability Office
GDP	Gross domestic product
ICS	Industrial control Systems
ICT	Information and communications technology
IEC	International Electrotechnical Commission
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
ISO	International Standards Organization
ISP	Internet service providers
IT	Information technology
ITC	Integrated Intelligence Center
ITL	Information Technology Laboratory
MSISAC	Multistate Information Sharing and Analysis Center
MTS	Marine transportation system
NCCIC	National Cyber Security and Communications Integration Center
NCSA	National Cyber Security Authority
NIST	National Institute of Science and Technology
OMB	Office of management and budget
POTW	Publically owned treatment works
PPDR	Public protection and disaster relief
PPP	Public private partnership
PWS	Public water system
SCADA	Supervisory control and data acquisition
TETRA	TErrestrial Trunked RAdio
TSP	Thrift savings plan
US	United States
US CERT	US Computer Emergency Readiness Team
V2X	Vehicle to X (infrastructure, vehicle)

1.1 Introduction

Challenges with cyber security have the potential for becoming one of the defining issues of our time. In 2009, the President of the United States (US) declared cyber-threats to be among "the most serious economic and national security challenges we face as a nation" and stated that "America's economic prosperity in the twenty-first century will depend on cyber-security." (Obama 2009). In January 2012, the US Director of National Intelligence testified before the Subcommittee on Oversight, Investigations, and Management, Committee on Homeland Security, House of Representatives that cyber-threats pose a critical national and economic security concern (Clapper 2012). To further highlight the importance of these threats, on October 11, 2012, the US Secretary of Defense stated that the collective result of attacks on our nation's critical infrastructure could be "a cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life." (Panetta 2012). The US Government Accountability Office (GAO) has conducted a number of studies attempting to highlight and document US vulnerability to cyber-threats. According to a 2013 report issued by the US GAO, cyber security threats to systems supporting critical infrastructure and federal information systems are evolving and growing (US GAO 2013). As will be discussed, these concerns apply to governments throughout the world.

In February 2013, the President of the US issued Executive Order 13636 with the intent of improving the cyber security of US critical infrastructure (CI) (Fischer et al. 2013). The order attempted to enhance the security and resiliency of US CI through voluntary, and collaborative efforts including

- expanding an existing Department of Homeland Security (DHS) program for information; sharing and collaboration between the government and the private sector;
- developing a process for identifying CI that have a high priority for protection;
- requiring the National Institute of Standards and Technology (NIST) to develop a Cybersecurity Framework of standards and best practices for protecting CI; and,
- Requiring regulatory agencies to determine the adequacy of current requirements and their authority to establish requirements to address the risks.

Cyber-threats to US infrastructure, and other assets, are of growing concern to policymakers. Information and communications technology (ICT) is becoming ubiquitous in the US and many ICT devices and other components are interdependent. Therefore, disruption of one component may have a negative, cascading effect on others. Cyber-attacks might include denial of service, theft or manipulation of data. Damage to critical infrastructure through a cyber-based attack could have a significant impact on national security, the economy, and the livelihood and safety of citizens. It is clear that cyber security issues include not only the threats associated with information technology but involve also physical threats to CI.

Commonly recognized cyber-aggressors include (Fischer et al. 2013).

- Cyber-terrorists who are state-sponsored and non-state actors who engage in cyber-attacks as a form of warfare.
- Cyber-spies stealing classified or proprietary information used by governments or private corporations to gain a competitive strategic, security, financial, or political advantage.
- Cyber-thieves engaged in illegal cyber-attacks for monetary gain.
- Cyber-warriors who are agents or quasi-agents of nation-states who develop capabilities and undertake cyber-attacks in support of a country's strategic objectives.
- Cyber-hacktivists who perform cyber-attacks for pleasure, or for philosophical or other nonmonetary reasons.

Even though cyber-threats pose a major threat to CI, in the US, the Federal role in what is now called cyber security has been debated for more than a decade. One of the reasons, action at the Federal level for protecting CI is limited lies in the political structure of the US. In the US, State and local governments have been the major institutions responsible for providing services to their populations. In addition, the US Constitution provides for a separation of powers between the States and the Federal government. Therefore, the National Governors Association (NGA), a non-partisan organization representing the interests of the 50 states and trust territories, is taking action in this important area. Governments in countries that do not have the political separation of power that exists in the US may therefore be able to adopt a more integrated approach to cyber security. Some of the problems caused by this dichotomy of responsibility as well as strategies used by other governments that have proven to be effective in dealing with cyber security challenges at the state, provincial and local levels, will be discussed in the following section.

1.2 Cyber Security Challenges

The US GAO has conducted a number of comprehensive studies on the vulnerability of US governmental and societal functions to cyber-threats. According to these studies, advanced persistent threats (APTs) pose increasing risks (US GAO 2011) in the US and throughout the world. APTs occur where adversaries possess sophisticated levels of expertise and significant resources to pursue their objectives repeatedly over an extended period of time. These objectives may be perpetrated by foreign militaries or organized international crime. Growing and evolving threats can potentially affect all segments of society including individuals, private businesses, government agencies, and other entities.

National threats to security include those aimed against governmental systems and networks including military systems, as well as against private companies that support government activities or control critical infrastructure (US GAO 2011). Threats to commerce and intellectual property including obtaining confidential

intellectual property of private companies and governments, or individuals with the aim of using that intellectual property for economic gain. Threats to individuals lead to the unauthorized disclosure of personally identifiable information, such as taxpayer data, Social Security numbers, credit and debit card information, or medical records. The disclosure of such information could cause harm to individuals, including identity theft, financial loss, and embarrassment.

Typical threats include the following (US GAO 2011):

- A bot-network operator which uses a network, or bot-net, of compromised, remotely controlled systems to coordinate attacks and to distribute phishing schemes, spam, and malware attacks.
- Criminal groups which attack systems for monetary gain. Specifically, organized criminal groups use spam, phishing, and spyware/malware to commit identity theft, online fraud, and computer extortion.
- International corporate spies and criminal organizations which conduct industrial espionage and large-scale monetary theft and to hire or develop hacker talent.
- Hackers who break into networks for the thrill of the challenge, bragging rights in the hacker community, revenge, stalking, monetary gain, and political activism, among other reasons. Hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Attack tools have become much more sophisticated, and easier to use.
- A disgruntled organization insider which is a principal source of computer crime. The insider threat includes contractors hired by the organization, as well as careless or poorly trained employees who may inadvertently introduce malware into systems.
- Nations which use cyber tools as part of their information-gathering and espionage activities.
- Phishers who are individuals or small groups that execute phishing schemes to steal identities or information for monetary gain. Phishers may also use spam and spyware or malware to accomplish their objectives.
- Spammers who are individuals or organizations that distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware or malware, or attack organizations (e.g., a denial of service).
- Spyware or malware authors who are individuals or organizations with malicious intent carrying out attacks against users by producing and distributing spyware and malware.
- Terrorists who seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence.

Cyber-based attacks can result in the loss of sensitive information and damage to economic and national security, the loss of privacy, identity theft, or the compromise of proprietary information or intellectual property. US Federal agencies have

reported that in the period between 2006 and 2012, the number of cyber security incidents has increased dramatically. According to the U.S. Computer Emergency Readiness Team (US-CERT), over this period, these incidents have increased from 5503 to 48,562; an increase of 782 % (US GAO 2013).

Based on US experience, the following examples from news media and other public sources illustrate that a broad array of information and assets remain at risk (US GAO 2013):

- In 2008, confidential information of the US Department of Defense (DOD) was successfully compromised when an infected flash drive was inserted into a US military laptop at a military base in the Middle East. The flash drive contained malicious computer code, placed there by a foreign intelligence agency that uploaded itself onto the military network, spreading through classified and unclassified systems. According to the Deputy Secretary of Defense, this incident was the most significant breach of US military computers at that time. This breach obtained information about network authentication tokens for a US military contractor. In May 2011, attackers used this information to make duplicate network authentication tokens and breached the contractor's security systems containing sensitive weapons information and military technology.
- In mid-2009, a research chemist with DuPont Corporation downloaded proprietary information to a personal e-mail account and thumb drive with the intention of transferring this information to Peking University in China. The chemist also sought Chinese government funding to commercialize research related to the information he had stolen.
- In March 2011, an individual was found guilty of distributing source code stolen from his employer, an American company. The investigation revealed that a Chinese company paid the individual $1.5 million to create a control system source code based on the American company's design.
- In February 2012, the US National Aeronautics and Space Administration (NASA) inspector general testified that computers with Chinese-based Internet protocol addresses had gained full access to key systems at its Jet Propulsion Laboratory. This access enabled attackers to modify, copy, or delete sensitive files; create user accounts for mission-critical laboratory systems; and upload hacking tools to steal user credentials and compromise other NASA systems (Martin 2012).
- In March 2012, attackers breached a server that held thousands of Medicaid records at the Utah Department of Health (USA). Included in the breach were the names of Medicaid recipients and clients of the Children's Health Insurance Plan. In addition, approximately 280,000 people had their Social Security numbers exposed. As a result of the attack, approximately 123,000 people who participated in the US Government's Thrift Saving Plan (TSP) had their personal information accessed. According to the board, the information included 43,587 individuals' names, addresses, and Social Security numbers; and 79,614 individuals' Social Security numbers and other TSP-related information.

350,000 people listed in the eligibility inquiries may have had other sensitive data stolen, including names, birth dates, and addresses.

- In March 2012, Global Payments, a credit-transaction processor in Atlanta, reported a data breach that exposed credit and debit card account information of as many as 1.5 million accounts in North America. Although Global Payments did not believe any personal information was taken, it provided alerts and planned to pay for credit monitoring for those whose personal information was at risk.

Three dramatic examples that illustrate the potential for cyber-attacks against critical infrastructure are as follows:

- Stuxnet, the malware which slowly damaged the centrifuges at Natanz nuclear enrichment facilities in Iran. It reprogrammed the Programmable Logic Controllers (PLCs) that controlled the centrifuges and caused them to spin out of control. To accomplish that goal, it had to propagate stealthily inside air-gapped networks. It is estimated that the malware probably had been implanted in late 2007; and by the end of 2010, the worm had infected approximately 100,000 hosts in dozens of countries (Janke et al. 2014).
- A city within the Australian state of Queensland (Maroochy Shire) found that a computer expert who had been rejected for a job with local government decided to seek revenge by hacking into the city's wastewater management system. During a two-month period, he directed computers to spill hundreds of thousands of gallons of raw sewage into local rivers, parks, and public areas before authorities were able to identify him as the perpetrator (Janke et al. 2014).
- In Eastern Ukraine in late December, 2015 power was cut to more than 600,000 homes and Russia was identified as the likely source of the attack. Ukraine's security service and government blamed Russia for the attack. Experts at the CIA, National Security Agency, and the Department of Homeland Security are investigating whether samples of malware recovered from the company's network indicate that the blackout was caused by hacking and whether it can be traced back to Russia. Researchers from a private global security company claimed they had samples of the malicious code that affected three of the region's power companies, causing "destructive events." The group behind the attack has been identified as the "the Sandworm gang," which is believed to have targeted NATO, Ukraine, Poland, and European industries in 2014 (http://qz.com/587520/russian-hackers-are-suspected-in-a-cyber-attack-that-caused-a-huge-blackout-in-ukraine/ accessed Feb 11, 2016)

Cyber-attacks have become an ever-increasing threat and the FBI ranks cybercrime as one of its most important law enforcement activities. President Barack Obama's recently proposed budget would sharply increase annual spending on cyber security, from $13 to $14 billion (http://www.techinsider.io/cyberattacks-2015-12 accessed on March 7, 2016; http://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html?_r=0 accessed on March 7, 2016).

1.2.1 US Federal Information Security Responsibilities as Established in Law and Policy

In the United States, the Federal Information Security Management Act (FIMSA) of 2002 assigns specific cyber security responsibilities to agencies such as the Office of Management and Budget (OMB), the National Institute of Science and Technology (NIST), and Inspectors General (US GAO 2013). FISMA requires each agency to develop, document, and implement an information security program to include, among other things, a comprehensive risk-based framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. Other laws give federal agencies general responsibilities that can include cyber security-related duties. For example, the Federal Bureau of Investigation (FBI) is responsible for detecting and prosecuting crimes which can include cybercrimes. Other laws address national security responsibilities including national defense and intelligence agencies, and can also include cyber-related threats to national security.

NIST's responsibilities under FISMA is to develop security standards and guidelines including the following:

- standards for categorizing information and information systems according to ranges of risk levels;
- minimum security requirements for information and information systems in risk categories;
- guidelines for detection and handling of information security incidents; and,
- Guidelines for identifying an information system as a national security system.

NIST standards and guidelines, like OMB policies, do not apply to national security systems.

(Title III 2002). NIST also has related responsibilities under the Cyber Security Research and Development Act that includes developing a checklist of settings and option selections to minimize security risks associated with computer hardware and software widely used within the federal government (Pub. L. No. 107-305).

FISMA also requires each agency inspector general to annually evaluate the information security program and practices of the agency. The Department of Homeland Security (DHS) has been assigned five specific responsibilities by OMB under FISMA (US GAO 2013)

- overseeing and assisting government efforts to provide adequate, risk-based, and cost-effective cyber security;
- overseeing agencies' compliance with FISMA;
- overseeing agencies' cyber security operations and incident response; and
- reviewing annual cyber security programs of agencies.

A number of directives and legislative actions have been issued by the US Government related to cyber security. Federal agencies have been given responsibilities related to the protection of critical infrastructures, which are largely owned by the private sector and local government.

1.2.2 Evolution of US Federal Strategy

Although the US federal strategy to address cyber security issues has been described in a number of documents, no integrated, overarching strategy has yet been developed (US GAO 2013). Without an overarching strategy, the government has limited ability to determine the progress it has made in reaching its objectives and to hold key organizations accountable for carrying out planned activities (US GAO 2013).

The US Federal role in what is now called cyber security has been debated for more than a decade but because of the political structure of the US, the role of the Federal sector is limited and must be carefully approached.

In an attempt to bridge the constitutional issues that exist in the US, the National Governors Association (NGA) has taken a major step forward in addressing cyber security issues. The NGA is an organization consisting of the governors of the states, territories, and commonwealths of the United States, founded in 1908. It is the bipartisan organization of the nation's governors and acts for the governors on matters of national policy, as well as allowing governors to share best practices and coordinate inter-state initiatives. Through the NGA, governors can speak with a collective voice on national policy and develop innovative solutions that improve state government and support the principles of federalism (http://www.nga.org/cms/about). Recently, the NGA has focused on cyber security issues at the state and local level.

1.3 Activities of the US National Governors Association

In the diverse services supplied by State and local level government, many are vulnerable to cyber-threats. Therefore, the NGA has released a statement on the importance of cyberspace security in protecting the ability of federal, state, and local governments to perform their vital functions (Crouch and McKee 2011). According to the statement "Due to the breadth and scope of the state role in entitlement services, facilitating travel and commerce, regulatory oversight, licensing and citizen services, states gather, process, store and share extensive amounts of personal information. From cradle to grave, the states are the nexus of identity information for individuals. This makes the states prime targets for external and internal cyber threats." State and local governments administer many programs that are funded by the federal government.

The use of web technologies, to facilitate government services, has caused the number of vulnerable services to rise. Crouch and McKee (2011) provided a series of examples that illustrate the vulnerability of state and local services to cyber-attacks. For example:

- The Internet is increasingly being used to renew drivers' licenses, vehicle registration, voting in elections, payment of utility bills, and registering for locally provided recreation activities.

- First responders provided by city county and state governments such as firemen, police, ambulance services, and the National Guard, are frequently dependent on cyber-based technologies to communicate and execute key command and control responsibilities.
- In November of 2010, hackers believed to be from Russia stole $200,000 in electronic fund transfers intended for schools and cities in Gregg County, Texas. It is believed that a county computer became infected with the Zeus Trojan "King of the Bots" disseminated via e-mail. Gregg County has reverted to a system of paper checks and deposit slips to transfer funds.
- In July 2010, Poplar Bluff, Missouri, experienced an increase (from 500 to 45,000 per week) in attempts by hackers to disrupt municipal utility services and these higher numbers have continued. The city requested the FBI to investigate the matter.
- In April 2010, in Morgan Hill California Hill, approximately 70 miles south of San Francisco, attackers climbed down manholes within the city, cut eight fiber cables causing a massive disruption in Morgan Hill and parts of three surrounding counties. The attack resulted in the loss of emergency 911 service, cellular telephone capability, land-line telephone, digital subscriber line (DSL) internet and private networks, central station fire and burglar alarms, automated teller machines (ATMs), credit card terminals, and monitoring of critical utilities.
- Based on an audit conducted by the state of Colorado it is estimated that there had been 43 cyber security incidents reported to the state from 2006 to 2010. Auditors believed the number was higher, and that some known incidents had not been reported.

The NGA has, therefore, identified cyber security as a major issue for governors to address at the state and local level. A white paper issued by the NGA has highlighted actions that governors can take to protect states and local governments from the growing number and sophisticated attacks against communication networks and systems. These systems include data bases containing sensitive and private information; financial, payment and tax systems and other critical cyber infrastructure (Saporito 2014).

Saporito (2014) recommends that the various States take the following steps:

- For the near term, develop a strategy to defend the State's cyber security assets. This step would include
  - Developing a strategic understanding of the state's cyber security risk profile, including current threats and the existing workforce capacity.
  - Deciding whether to train, hire or contract out cyber security management.
  - Evaluating state employees' capacity to provide cyber security.

    Assess the state's cyber security workforce supply by surveying job postings, wage and salary data, and state employees.

Improve retention and quality of the workforce through human resource policies and training.

- Future Activities
  - For the long term, align state education and workforce programs to support training of cyber security workers.
  - Designate computer science as a Science, technology, engineering and mathematics (STEM) course.
  - Assess the capacity of educators and schools to meet the needs of the cyber security workforce.
  - Use the community college system to educate students for the various cyber security tasks.
  - Employ partnerships with academic institutions and the private sector.

According to Saporito (2014) if the governors follow the above short, and long-term recommendations they can make significant strides addressing cyber security challenges. The NGA has also taken the lead in creating fusion centers which are owned and operated by state and local governments and serve as focal points for state, local, federal, tribal, and territorial partners to receive, analyze, and share threat-related information (Blute 2015). Fusion centers were created in the wake of 9/11 to facilitate information sharing among public safety agencies to prevent terror incidents, protect citizens, and respond to crises. There are in 2016, 78 centers, 53 of which are owned and operated by states and territories and 25 by major urban areas. Fusion centers are generally staffed by professionals from law enforcement, homeland security, fire, emergency response, public health services, and representatives of the private sector. They have focused on areas such as counterterrorism, disaster management, emergency response, protection of critical infrastructure, and drug trafficking. Fusion centers are organizationally distinct, but efforts are underway to better align and encourage mutual support across all of the nation's fusion centers. Those efforts aim to develop strategies to bridge jurisdictional boundaries as well as provide more effective communications about and effective response to the threat environment.

Some other organizations that can assist in the cyber security effort are (Saporito 2014):

- Information sharing and analysis organizations (ISAOs) which are organizations created to share and analyze information related to emerging cyber-threats and cyber vulnerabilities.
- Sector-specific information sharing and analysis centers (ISACs) which are entities created by owner-operators of critical infrastructure to help facilitate information sharing within those sectors. They provide risk mitigation, incident response, alert, and information sharing.
- The Multi-State Information Sharing and Analysis Center (MSISAC) helps collect, share, and analyze cyber security information with states.

- The Integrated Intelligence Center (IIC) which has the goal of ensuring that actionable information pertaining to cyber security is disseminated and shared with fusion centers in a timely fashion.
- The National Cybersecurity and Communications Integration Center (NCCIC) which provides ongoing cyber situational awareness, incident response, and management to the federal government, intelligence community, and law enforcement. Its mission is "to reduce the likelihood and severity of incidents that may significantly compromise the security and resilience of the Nation's critical information technology and communications networks.

There are obviously many research studies being conducted and much research underway devoted to understanding and protecting against the vulnerability of state, municipal, provincial, and local government to cyber-attacks. Some of these studies are discussed in the following sections.

1.4 US Cyber-Security Research

There are clearly many issues related to the vulnerability of critical infrastructure to cyber-attacks in the US. This book contains contributions from a number of cutting-edge researchers and specialists who are attempting to address these important issues.

Alexander and Panguluri (Chap. 2, this volume) discuss some of the complex terminology and institutional relationships involved in developing a program to improve an organization's security position. They also discuss three published standards which have been developed to establish an effective program to protect against cyber-threats. The authors emphasize the concept that there are many existing resources which can be applied to cyber security problems so that it is not necessary to start with an entirely blank sheet.

Scott White (Chap. 3, this volume) examines both municipal cyber security infrastructure and the threats facing municipalities. Cyber-attacks include the unintentional or unauthorized access, use, manipulation, interruption or destruction of electronic information and/or the electronic and physical infrastructure used to process, communicate, and store that information. Cyber-attackers can disrupt the electronic controls of power grids, water treatment plants, and telecommunications networks and can interfere with the production and delivery of basic goods and services provided by municipal governments. All municipalities must maintain constant vigilance and must strengthen their capability to detect, deter, and defend against cyber-attacks.

Ginter (Chap. 4, this volume) examines the history and evolution of perimeter protection for control system networks, modern threats, and attacks. He explains the limitations of information technology (IT)-centric protections, and the unidirectional protections being deployed increasingly at all types of industrial sites. Industrial control system networks are used to control the physical processes

essential to water treatment and distribution systems, electric generation, transmission and distribution systems, manufacturing systems, as well as, petrochemical pipelines and many other industrial processes. The author suggests the use of unidirectional gateways as a strong protection against remote-control, targeted attacks. At this writing, many industrial process owners and operators have already deployed unidirectional protections, but many more have not.

Stern (Chap. 5, this volume) presents a case study involving the City of Pittsburgh and the H. John Heinz III College at Carnegie Mellon University in which the organizations collaborated to identify a major vulnerability in the City's computer systems. As a motivation for the collaboration, an unknown prankster thought it would be amusing to replace the words "City of Pittsburgh" with a few choice obscenities in every outgoing real estate tax bill. The prankster was able to penetrate the City's existing firewall and globally insert the off-color language without being detected by network administrators. The City's Chief Information Officer (CIO) decided to reach out to one of the City's academic partners, Carnegie Mellon University (CMU), to help the City conduct a security audit of its computer network. The CMU students identified numerous security breaches for the City while obtaining an invaluable real-world learning experience. This innovative collaboration can serve as a model for future government–university partnerships.

Tucci (Chap. 6, this volume) discusses the vulnerability of the, often overlooked, Marine Transportation System (MTS) to cyber-attacks. The MTS is a major component of the world's overall transportation and energy system. It is a dominant factor in the global supply chain that connects businesses and individuals all over the world. U.S. economic prosperity is highly dependent upon maritime trade and the ships, boats, terminals, and related maritime critical infrastructure that support their many tributaries. According to the U.S. Maritime Administration, waterborne cargo and associated activities contribute more than $649 billion to the U.S. Gross Domestic Product (GDP) sustaining more than 13 million jobs. Many thousands of vessels, from tugs and barges to ocean going ships complete this system. By volume, over 90 % of U.S. overseas trade travels by water. The US Coast Guard and other authorities have documented cyber-related impacts on technologies ranging from container terminal operations ashore to offshore platform stability and dynamic positioning systems for offshore supply vessels.

Panguluri et al. (Chap. 7, this volume) discuss the cyber vulnerabilities of public water and wastewater water utilities. From a public health and an economic perceptive, both water and wastewater utilities represent critical infrastructures that must be protected. SCADA/ICS systems are an essential component for the effective operation of medium-to-large water and wastewater utilities. It is imperative that the PWSs and POTWs adopt suitable countermeasures to prevent or minimize the consequences of cyber-attacks. A sector-specific secure design example is provided by the authors to guide PWSs and POTWs in refining their approach to cyber security.

Gregg White (Chap. 8, this volume) discusses an effort to help states and communities build viable and sustainable cyber security programs. The cyber threat is becoming increasingly sophisticated, attacks are more targeted and are occurring

more often than in the past. Everyone is vulnerable to a cyber incident whether they are directly targeted in a cyber-attack or the victim of a data breach. The attackers no longer need to be in the local proximity of the incident, now they can be anywhere in the world, which makes it much harder to identify and locate who is behind the cyber-attack or cyber event. The Community Cyber Security Maturity Model (CCSMM) was developed to address this specific issue.

1.5 International Studies and Research on Cyber-Physical Security

Cyber-security, as has been discussed, at the local and municipal level is not only a problem in the US, it is an international issue as well as discussed in the following paragraphs.

Boes and Leukfeldt (Chap. 9, this volume) describe the fight against cybercrime from a European perspective. Safety is a public good, which can be threatened by crime and safety, and should be guaranteed in both the offline and cyberspace worlds. A possible strategy to overcome such problems is an approach, in which all relevant stakeholders—public as well as private—participate in (the implementation of) safety and security policy. A clear strategy that should be investigated is the development of public–private partnerships (PPPs). A Dutch PPP established within the field of cybercrime is described in-depth.

According to Tabansky (Chap. 10, this volume) Israel perceives cyber security as intrinsically integrated with physical security. To mitigate cyber-physical risk, a centralized civilian Critical Infrastructure Protection (CIP) regulation was enacted in Israel in 2002. The Israeli experience demonstrates that comprehensive cyber-physical security depends on the political ability to reach an acceptable balance between competing values among various stakeholders in the public and business sector, while maintaining information technical (IT)-security capacity. Water security is used as an excellent example of the need to maintain that balance.

According to Jiow (Chap. 11, this volume) critical infrastructure, such as transportation networks, electricity generation distribution networks, sophisticated communication systems, water and gas distribution networks, has increasingly relied on the Internet and networked connections for its operations. These systems are frequently referred to as cyber-physical (CP) Systems. Most discussion focuses on technological solutions and fixes as a means of protecting CP systems. A frequently overlooked aspect of CP protection, is the application of educational efforts to cultivate safe online practices. Two case studies based on experience in Australia and Singapore are explored.

Rajamäki (Chap. 12, this volume) discusses the increased need for European collaboration and information sharing related to CIP. He makes the important case that public protection and disaster relief (PPDR) communications and information exchange technologies and procedure are part of the critical infrastructure. These

functions are increasingly dependent on networks, and data processing infrastructure. The author believes cyber security should be seen as a key enabler for the development and maintenance of trust in the digital world. Rather than thinking of "cyber- security as a barrier" to new interactions and services it is possible that "cyber-security as an enabler" of new interactions and services.

Alazab and Broadhurst (Chap. 13, this volume) describe the nature and trends in spam borne malware and outline some of the issues and problems with respect to it as a cybercrime. It is predicted that will be 25 billion devices connected to the Internet by 2015 and 50 billion by 2020. This connectivity has the potential of affecting everyone, especially with the growing use of mobile devices, cloud computing, and a network of networks. Spam emails and cloaked phishing sites are blending with malware tools to enhance the ease of identity theft. Spam as a cybercrime, takes many forms and many varieties have been described in a European Commission study. One recent study of spam and phishing identified the location of high risk internet service providers (ISPs) that acted as "Internet bad neighbours", and found that spam originates from a small number of ISPs.

Oka (Chap. 14, this volume) focuses on automotive security, and describes cyber security attacks targeting vehicles and their infrastructure. With the emergence of the *connected car*, there is a clear need for cyber security solutions within the automotive industry and within transportation systems. Automotive security advancements such as automotive-grade hardware security modules, secure vehicle-to-X (V2X, i.e., vehicle-to-vehicle and vehicle-to-infrastructure) communications, secure in-vehicle communications, and embedded security evaluations of automotive components are explored.

1.6 Summary and Conclusions

The issue of cyber-security is currently having and will continue to have an impact on organized society throughout the world. It is important that national governments develop comprehensive strategies to deal with issues related to cyber-security. In addition, as infrastructure becomes increasingly connected and capable of communicating, cyber-physical security at the Provincial, State, local, and municipal level has and is becoming an international problem. In the US, cyber-security issues have become extremely important from a national security perspective (US GAO 2013). However, in the US the constitutions requirement for separation of powers between the Federal government and the individual States has made developing a unified cyber security strategy very difficult. To deal with this issue in the US, the NGA has identified cyber security as a major issue for governors to address at the state and local level. Other developed and developing countries have dealt with this problem in a more "seamless" manner using for example, PPPs. As critical infrastructure becomes more dependent on computer technology and increasingly tied to the internet, cyber-attacks against communication networks and system are growing in number and are becoming more

sophisticated. Several examples are presented, in this book, that illustrate the impact of cyber-attacks on National security as well as attacks on critical infrastructure.

A number of important issues related to cyber security and the fundamental provision of services at the local level, have been discussed including the development of specialized terminology and standards that relate to cyber security. It has become traditional to construct "firewalls" to protect computer systems. Firewalls are essentially software systems but there is a growing application of unidirectional gateways which provide "hardware" solutions to protect critical infrastructure. Education is also a key component of protecting against cyber-threats and is also an important aspect of cyber security. It should include not only government and private sector organizations but individual users as well. There is clearly an increased need for collaboration and information sharing related to CIP and PPDR communications and information exchange technologies and procedures. Rather than thinking of "cyber- security as a barrier" to new interactions and services it is possible to think of "cyber-security as an enabler" of new interactions and services and the development of "trust" in the user community. Spam malware is an important and pervasive cybercrime and it is important to understand some of its issues and problems and to treat it as a cybercrime. Virtually everyone who uses a computer is affected by spam. A newly emerging cyber vulnerability is the growing area of vehicle-to-vehicle and vehicle-to-infrastructure communications. This emerging technology has the potential for being highly vulnerable to cyber-attack.

Several studies are presented that illustrate the vulnerability of critical infrastructure to cyber-attack. These case studies include: the City of Pittsburgh and its work with Carnegie Mellon University in an attempt to provide security to city services; the MTS which is a frequently overlooked but absolutely critical local and/or municipal service; publically owned treatment works and public water supplies including an example of the potential application of unidirectional gateways. An effort to help states and communities build viable and sustainable cyber security programs to address local and municipal cyber security threats is being suggested through the development of the CCSMM.

Examples of the fight against cybercrime from an international perspective is described and an approach suggested, in which all relevant stakeholders—public as well as private—participate in the development of PPPs. In Israel in an effort to mitigate cyber-physical risk a centralized civilian CIP regulation was enacted in 2002.

It is clear that the issues of cyber-security and the vulnerability of individuals, local and national government and private parties to cyber-attacks is, and will continue to be one of the defining issues of our time. The author's believe that there are a number of steps that could be taken to address the vulnerabilities of critical infrastructure to cyber-physical attacks. Many of these steps are discussed in this book. For example, from a technical perspective, computer science educators should introduce cyber-security as part of the teaching syllabus. Broader education programs could be launched for the general public including the need for secure passwords and the need to be aware of the dangers of spam. Continuous improvement in fire walls should be pursued and very promising technological

solutions such as unidirectional gateways should be implemented. A promising solution to providing cyber-security at a strategic level is the adoption of public–private partnerships (PPPs). PPPs have the potential for solving some of the constitutional and political barriers in the US and the concern for separation of national and local functions in Israel.

The authors wish to applaud the many dedicated professionals working to find solutions to the problem of critical infrastructure protection throughout the world. Hopefully, this book will help in some small measure to support their important efforts.

References

Accessed on February 11, 2016 from http://qz.com/587520/russian-hackers-are-suspected-in-a-cyber-attack-that-caused-a-huge-blackout-in-ukraine/

Accessed on December 17, 2015 from http://www.nga.org/cms/about

Accessed on March 7, 2016 from http://www.techinsider.io/cyberattacks-2015-12

Accessed on March 7, 2016 from http://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html?_r=0

Blute, T. (2015). Enhancing the role of fusion centers in cybersecurity. Washington, D.C.

Clapper, J. R. (2012, January 31). Director of National Intelligence. Unclassified statement for the record on the worldwide threat assessment of the US intelligence community for the senate select committee on intelligence.

Crouch, J. E., & McKee, L. K. Jr., (2011, February 25). Cybersecurity at the state and municipality levels where do we stand? In *Improving the Future of Cyberspace…Issues, Ideas, Answers. NSCI, 2011*. 110 Royal Aberdeen. Smithfield, VA.

Fischer, E. A., Liu, E. C., Rollins, J., & Theohary, C. A. (2013, March 1). The 2013 cybersecurity executive order: Overview and considerations for congress. Congressional Research Service, 7-5700. www.crs.gov

Janke, R., Tryby, M. E., & Clark, R. M. (2014). Protecting water supply critical infrastructure: An overview. In M. C. Robert & S. Hakim (Eds.), *Securing water and wastewater systems: Global experiences.* Switzerland: Springer.

Martin, P. K. (2012, February 29). Inspector General, National Aeronautics and Space Administration. NASA cybersecurity: An examination of the agency's information security. testimony before the Subcommittee on Investigations and Oversight, Committee on Science, Space, and Technology, House of Representatives, Washington, D.C.

Obama, B. (2009, May 29) Remarks by the President on Securing Our Nation's Cyber Infrastructure, Washington, D.C.

Panetta, L. E. (2012, October 11). Secretary of Defense, Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City.

Pub. L. No. 107-305 (2002, November 27). 15 U.S.C.§ 7406(c)

Saporito, L. (2014, October 27). *The cybersecurity workforce: States' needs and opportunities*. Washington, DC: National Governors Association Center for Best Practices.

Title III of the E-Government Act of 2002, Pub. L. No. 107-347, December 17, 2002; 44 U.S.C 3541.

United States Government Accountability Office (GAO). (2011, February). High risk series: An update, GAO-11-278, Washington, D.C.

United States Government Accountability Office (GAO). (2013 February). Cybersecurity national strategy, roles, and responsibilities need to be better defined and more effectively implemented, GAO-13-187.

Chapter 2
Cybersecurity Terminology and Frameworks

Richard D. Alexander and Srinivas Panguluri

Abstract The documents related to cybersecurity are often filled with information technology (IT) acronyms and with familiar business terms that need to be understood in the context of cybersecurity. In order to develop and implement an effective cybersecurity program, it is necessary to understand the terminology and its contextual use. Cybersecurity programs often evolve within an organization and, depending on the history of that evolution, the implemented measures may be somewhat unbalanced. For example, in some organizations the program may be headed by an IT professional who has exceptional IT skills, so she or he may place an emphasis on technical controls such as firewalls and authentication measures and the resulting program may not have enough administrative controls in place. Any organization can improve their cybersecurity posture by taking a balanced approach. A balance can be reached by utilizing a framework that allows a cybersecurity program to document its programmatic strengths and weaknesses thus hopefully achieving a better balance over time. This chapter defines key cybersecurity terminology and discusses three popular standards/frameworks that are very relevant to cybersecurity in the critical infrastructure sector. Specifically, the information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) under the ISO/IEC 27000 series is discussed, followed by a summary of the National Institute of Standards and Technology (NIST) Cybersecurity Framework for Critical Infrastructure and the NIST Special Publication 800-82—A Guide to Industrial Control Systems (ICS) Security, both of which have direct relevance to many of the various critical infrastructure sectors in the U.S.

R.D. Alexander (✉)
Interlynx Group LLC, PO Box 36167, Cincinnati, OH 45236, USA
e-mail: Richard.Alexander@interlynx.org

S. Panguluri
CB&I Federal Services LLC, 5050 Section Avenue, Cincinnati, OH 45212, USA
e-mail: Srinivas.Panguluri@cbifederalservices.com

R.M. Clark and S. Hakim (eds.), *Cyber-Physical Security*,
Protecting Critical Infrastructure 3, DOI 10.1007/978-3-319-32824-9_2

Acronyms

ABAC	Attribute based access control
AES	Advanced Encryption Standard
CIA	Confidentiality, integrity and availability
CRC	Cyclic redundancy checks
CSD	Computer security division
CSRC	Computer Security Resource Center
DCS	Distributed control systems
DNS	Domain name system
DMZ	De-militarized zone
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
HSPD-7	Homeland Security Presidential Directive 7
ICS	Industrial control systems
IDS	Intrusion detection system
IDPS	Intrusion detection and prevention systems
IEDs	Intelligent electronic devices
IEC	International Electrotechnical Commission
IP	Internet protocol
IPSec	Internet Protocol security
ISO	International Organization for Standardization
ISMS	Information Security management systems
IT	Information Technology
ITL	Information Technology Laboratory
NIST	National Institute of Standards and Technology
NISTIRs	NIST Interagency or Internal Reports
PII	Personally identifiable information
PIV	Personal identity verification
PLC	Programmable logic controllers
RAID	Redundant array of independent disks
SCADA	Supervisory control and data acquisition
SP	Special publication
U.S.	United States
WLANs	Wireless Local Area Networks

2.1 Introduction

The challenges involved in improving an organization's security posture can at times seem overwhelming. Thankfully, there are resources available which ensure that it is not necessary to start with an entirely blank sheet of paper. By leveraging a

selection of existing resources, an organization can avoid "reinvention of the wheel" and accelerate progress towards an improved security posture.

In this chapter, we examine a number of published standards and framework resources which are available to organizations. We consider a number of sources from the widely applicable ISO 27001 (ISO/IEC 2013b) standard whose various versions have spanned over a decade through to the more recent NIST "Framework for Improving Critical Infrastructure Cybersecurity" published in February 2014, (NIST 2014) and Revision 2 of the NIST 800-82 standard "Guide to Industrial Control Systems Security" published in May 2015 (NIST 2015).

We provide an overview of what is covered by each resource, how they inter-relate and consider how an organization can use these resources to accelerate its own understanding of its current security posture. This understanding can be leveraged to chart a course to their desired security posture and by identifying and prioritizing the improvements necessary to achieve that transition. To aid an understanding of all these resources, we first define some of the typical terminology used in the field of cybersecurity.

2.2 Terminology

2.2.1 Core Terminology

Before considering the standards themselves, it is useful to review the terminology which (with occasional nuanced variations in emphasis) is common to the standards. Some of the terminologies will be familiar from everyday usage but may take on a more particular meaning in the context of cybersecurity.

2.2.2 Scope

The process of improving an organization's cybersecurity can be considered as a continuous project and, like all projects, to be successful it is necessary to establish the project's scope. It is not uncommon to find that an organization may not initially have the resources or experience to address a wide cybersecurity scope. In such cases, it may be considered prudent to concentrate initially on those areas where the risks are perceived to be greatest and subsequently widen the scope as resources and experience permit. Note however that it is important to ensure that limited resources do indeed target areas of highest risk, so the process of determining those areas will serve the organization best if it is carried out formally and in a manner which encourages the widespread input of viewpoints.

2.2.3 Assets

This term may be familiar from its use in financial contexts. In the context of cybersecurity, the term refers to any organizational information resource that may be subject to cyber-attack and which is therefore in need of protection. The term can cover a wide range of resources such as data resources, software, physical computer systems, networks, utilities, and even less tangible resources such as reputation or community standing.

Critical infrastructure organizations share many of the same information assets as other business types and may also have additional assets specific to their specialty such as process plant, process controls, and associated software.

A common approach to defining the scope of a particular cybersecurity system is to decide which information assets are included and which are excluded. Clearly, in the long run, it is desirable to protect as many assets as is practical and cost-effective. For an organization that is just starting to grapple with cybersecurity, it may be preferable to ensure that an initial project addressing the most risk-critical information assets is successful before widening the scope of the endeavor.

In the context of cyber security, the information assets may have one or more security requirements. The three most common requirements are those typically referred to as confidentiality, integrity, and availability.

2.2.4 Confidentiality

Confidentiality of an information asset refers to the asset (or its contents) only being known to those authorized by the asset owner. Examples of information assets to be protected could be proprietary information, customer data, and employee data. For example, confidentiality of stored data might be achieved by implementing encryption of an individual file containing the data, the database, or the entire disk. For example, BitLocker is a full-disk encryption tool built into the Windows operating system.[1] It supports Advanced Encryption Standard (AES) 128-and 256-bit encryption, and it is primarily used for whole-disk encryption. The higher the bit level of encryption, the harder it is to break. Similarly, confidentiality of data can be protected during transmission by enforcing data encryption protocols such as the Internet Protocol Security (IPsec). IPSec is an Internet Protocol (IP) suite for securing communications by authenticating and encrypting each IP packet of a communication session.

[1]Windows is a family of graphical operating systems developed, marketed, and sold by Microsoft. Bitlocker is built into Windows 7 (Ultimate and Enterprise Versions) and Windows 8 (Pro and Enterprise), as well as the Windows Server operating systems (2008 and later).

2.2.5 Integrity

The integrity of an asset is adversely affected if the asset is altered incorrectly. For example, the information contained in a database may be altered by accidental corruption (perhaps due to partial storage failure) or by the deliberate unauthorized actions of an individual or individuals. Whether the cause is accidental or deliberate, protecting the integrity of an information asset from unauthorized or unintended modification is an essential component of cyber security. For example, a customer can be overcharged if the integrity of billing information is not protected. A cyber-attacker might compromise system integrity leading to unintended operations of pumps and valves resulting in damage to both information and non-information assets. Integrity at the source can be protected by implementing access controls, process controls, and configuration management. Integrity during data transmission can be achieved by implementing hashing algorithms or cyclic redundancy checks (CRC) to detect corruption.

2.2.6 Availability

The availability of an information asset is the ability to provide reliable and timely access to information assets to authorized individuals. For example, redundant array of independent disks (RAID) technology is commonly used in data storage to combine multiple hard-drive components into a single logical unit. If one hard drive

Fig. 2.1 Cybersecurity goal

fails, the data is still available for use. Computer networks and system have a plethora of equipment and software that must all work in concert to ensure the data is available to authorized individuals.

At its core, the goal of a cyber security program is to provide the required confidentiality, integrity and availability (CIA) protection to the information assets of the organization. Figure 2.1 is a graphical representation of this cyber security goal.

2.3 Risk Assessment Terminology

2.3.1 Threats

Threats to the organization's cyber security-related assets can come from a variety of sources. At one level, we can split these threat sources under two primary headings, those arising from people and those arising elsewhere.

2.3.1.1 Threats from People

A variety of people may be considered as threat sources. They may be internal or external to the organization and they may be known or unknown to the organization itself. When considering threats it is often useful to group the threat sources. In the case of people-related threats a non-exhaustive list could be:

- Employees
- Customers
- Vendors
- Former Employees
- Black-hat hackers[2]

For people-based threat sources, groupings can be made according to criteria such as asset access, skills of the threat source, and motivation of the threat source. For example, an organization may determine that the threats it faces from general administrative staff are distinct from those faced from IT staff (due to different forms of access to assets and varying skill sets), in which case it may choose to further divide the "Employees" group into "General Employees" and "IT Employees". Grouping the threat sources in such a manner helps to simplify the subsequent processes of risk assessment and risk treatment.

[2]The use of the term hacker has varied over time. The term "black hat hacker" is used here to definitively identify those with both the required technical skills *and* malevolent intentions.

2.3.1.2 Threats from Other Sources

Non-people threat sources include many environmental factors such as fire, flood, temperature, adverse weather, or the availability of required utility services such as electricity and water.

2.3.2 Vulnerabilities

A vulnerability is a weakness in an asset's protections such that a threat source may be able to adversely affect the security requirements (confidentiality, integrity or availability) of an asset.

Consider a basic threat to an information asset such as a computer. A computer behind a locked door may be considered to be less likely to be stolen than one which is in an open area. In this case, the lack of a locked door is a vulnerability which may result in a breach of the asset's availability. Likewise, a locked but weak door may be considered to leave an asset more vulnerable than a locked sturdy door.

The foregoing simple example relates to physical security. In the field of cybersecurity, we often hear the term "vulnerability" used in the context of vulnerabilities found in software. While the detail is different, the premise is the same. A vulnerability is something that one or more threat sources can exploit to negatively impact the confidentiality, integrity or availability of an asset.

2.3.3 Probability

Determining the probability that an asset might be subject to a particular cybersecurity occurrence can be a difficult matter. In some cases, there may be relevant historical data which provides some quantitative input, e.g., the likelihood of earthquakes in a particular region. In other cases, it may be necessary to estimate probability in simple bands such as "low", "medium", and "high". While such banding might seem highly subjective, it nevertheless provides relevant information when it comes to the allocation of limited resources to gain the maximum improvement in cybersecurity posture.

2.3.4 Impact

When considering impact, the aim is to express the impact on the organization's business goals if a threat source successfully exploits an asset's vulnerabilities and negatively impacts its confidentiality, integrity or availability. Again, there may be

some cases where quantitative currency values can be assigned to impact whereas in other situations estimating the impact in bands such as “low”, “medium”, and “high” impact is more practical. For critical infrastructure organizations, the impact of certain events may extend well beyond its own borders and may be difficult to quantify in financial terms. In such cases, organizations may choose to mix quantitative and qualitative methods such as the creation of several bands each representing the number of customers which could be affected by a potential event and the degree to which they would be affected.

2.4 Risk Treatment Terminology

For each identified risk, an organization can consider a number of possible responses as discussed below.

2.4.1 Risk Acceptance

Risk acceptance typically occurs when the organization deems that there are no practical, cost-effective means of further reducing the probability or impact of an event occurrence and therefore decides to accept the residual risk.

2.4.2 Risk Avoidance

In order to truly avoid a risk, it is generally necessary to change the organization’s behavior in some manner such that the risk simply does not arise. An example would be ceasing a particular process because the associated risk was considered to be too high.

2.4.3 Risk Treatment/Risk Mitigation

Treating or mitigating risks is a cornerstone of cybersecurity. It involves applying one or more controls such that the overall risk to an asset (in terms of probability and impact) is within the organization’s tolerance levels. Some controls are specifically aimed at reducing probability whereas others may target impact. By using a combination of controls, both factors can often be reduced.

2.4.4 Risk Transfer

Anybody who has insurance is familiar with one example of risk transfer. In return for payments, a third-party organization agrees to pay out to cover a financial loss in the event of a particular occurrence. Risk transfer can indeed be a useful way of dealing with certain cyber security risks; however, it should be remembered that not all risks are financial in nature. For critical infrastructure organizations, it may for instance, be appropriate to reduce the impact of a theft-related event through risk transfer (i.e., insurance), but intangible assets such as the organization's goodwill and standing in the community may be more difficult or impossible to protect in a similar way.

2.5 Controls Terminology

2.5.1 Controls Overview

Controls are the means by which risk can be mitigated. Individual controls may reduce the probability of a particular cybersecurity occurrence or the impact of such an occurrence. Typically, to reduce both probability and impact of the occurrence multiple controls will be applied.

2.5.1.1 Types of Controls

The word "controls" tends to conjure up images of electromechanical devices, but in the cyber security context controls can take on many forms. Some examples of control types are shown in Table 2.1.

2.5.2 ISO 27001/ISO 27002

The ISO 27001 and ISO 27002 standards were first published in their 2002 versions. These standards are also collectively referred to (with others) as the ISO2700 standards, or ISO27k for short. The current versions at the time of writing are the 2013 versions (ISO/IEC 2013a, b). Prior to 2005, ISO 27001/27002 can trace its roots to earlier British standards under the BS7799 heading, so these standards have matured over many years.

Unless stated otherwise, references to ISO 27001 (ISO/IEC 2013b) or ISO 27002 (ISO/IEC 2013a) in this chapter refer to the 2013 versions of the standard.

A selection of the ISO 27000 family of standards is shown in Table 2.2.

Table 2.1 Example control types

Control type	Description
Directive controls	Directive controls may be administrative instruments such as policies, standards and procedures. An example of a directive control would be the creation of an Acceptable Use Policy for employee use of information resources
Preventive controls	A preventative control attempts to make the occurrence of a breach less likely by making it more difficult for the threat source to cause one. Examples are security guards, security fences, security training, firewalls and intrusion prevention systems
Detective controls	A detective control detects a security breach once it has occurred. Examples are intruder alarms, intrusion detection systems, system monitoring and log monitoring
Corrective controls	A corrective control reduces the effect of a security breach. An example is an anti-virus system isolating an infected file
Recovery controls	A recovery control aims to restore business operations after a security breach. An example of such a control is the creation of a Disaster Recovery Plan

Table 2.2 A selection of ISO/IEC cybersecurity standards

ISO standard number	Main focus of the standard
ISO/IEC 27000:2014	Information security management systems—overview and vocabulary
ISO/IEC 27001:2013	Information security management systems—requirements
ISO/IEC 27002:2013	Code of practice for information security controls
ISO/IEC 27003:2010	Information security management system implementation guidance
ISO/IEC 27004:2009	Information security management—measurement
ISO/IEC 27005:2011	Information security risk management
ISO/IEC 27006:2011	Requirements for bodies providing audit and certification of information security management systems
ISO/IEC 27007:2011	Guidelines for information security management systems auditing
ISO/IEC 27008:2011	Guidelines for auditors on information security controls
ISO/IEC 27031:2011	Guidelines for information and communication technology readiness for business continuity

ISO 27001 and ISO 27002 are designed to be used in tandem. ISO 27001 lays out the requirements for the implementation of an "Information Security Management Systems" (ISMS) compliant with the standard. Annex A of ISO

27001, lists 114 information security controls grouped under 14 control categories. These categories cover functional headings such as supplier relationships, compliance, system acquisition, etc. ISO 27002 provides a code of practice for information security controls and includes further implementation guidance for each of the controls found in ISO 27001 Annex A.

2.6 Requirements of the ISO 27001 Information Security Management System

ISO/IEC 27001 describes an Information Security Management System (ISMS) and details the steps involved in the establishment of such a system in sections 4 through 10 of the standard. Those steps are summarized below.

2.6.1 Context

Under the heading of "context" the organization is required to:

- Determine the external and internal issues which affect the organization as it carries out its business objectives.
- Determine the information security requirements of relevant interested parties.
- Determine the scope of the information security management system. The scope should consider the points above along with the organization's interfaces with and dependencies on other organizations with regards to the information processes.
- Establish, implement, and maintain an information security management system consistent with the above.

2.6.2 Interested Parties

The concept of "interested parties" was introduced in the 2013 version of ISO 27001. The standard requires that the organization identify "interested parties that are relevant to the information management security system and the requirements of these interested parties relevant to information security". This approach ensures that an organization is considering the expectations of a wide range of parties which may extend beyond the organization itself into other areas such as customers, vendors, government regulators, and other third parties with an interest in the organization's information security practices.

2.6.3 Leadership and Commitment

The requirements under this heading are designed to ensure:

- That the information security policies and objectives are consistent with and support the organization's strategic objectives.
- That information security processes are integral to the organization's processes.
- That the resources required for the information management system are available.
- That the importance of information security management is communicated and understood.
- That the objectives of the information security management system are met.
- That relevant organizational people are supported and capable of supporting the information security management system.
- That the information security management system is continually improved.
- That management charged with responsibilities for the ISMS are supported as they provide leadership in the operation of the ISMS.

2.6.4 Policy

Under policy, the senior management of the organization is required to establish an information security policy which:

- Is appropriate to the organization's business objectives.
- Defines information security objectives or a framework for setting the same.
- Commits to meeting relevant information security requirements.
- Commits to the continual improvement of the information security management system.
- Is available in document form.
- Is communicated within the organization.
- Is available to interested parties where appropriate.

In ISO 27001 as with other information security frameworks the definition, adoption, authorization, and resourcing of an information security policy by senior management (at the organizational governance level) is considered to be essential to the success of the cyber security endeavor.

The definition of policy may start with a high-level overview statement from the board regarding the organization's approach to cyber security, its alignment with business objectives, its role in meeting compliance requirements and the resources, roles and responsibilities allocated towards these objectives by the board. Authorities and responsibilities for further fleshing out the details in terms of standards, procedures, guidelines and further subpolicies will flow from the initial high-level policy statement. Taken together, all of these policies, standards,

procedures, and guidelines become the manual which guides stakeholders both in terms of what a particular policy says and what resources are available for carrying out related security measures.

2.6.5 Organizational Roles, Responsibilities, and Authorities

This section requires senior management to assign the responsibilities and authority for information security roles and to ensure that these assignments are widely communicated.

The standard also calls out two specific responsibilities to be assigned, namely:

- The responsibility for ensuring that the information security management system conforms to ISO 27001.
- The responsibility for reporting to senior management on the performance of the information security management system.

2.6.6 Planning

2.6.6.1 Actions to Address Risks and Opportunities

Under the planning heading, ISO 27001 requires the organization to consider the organizational context and the information security requirements of interested parties (as identified under the Context heading above) and to identify and address the risks and opportunities which could impact the ability of the ISMS to achieve its objectives, achieve continual improvement or prevent or reduce undesired effects.

The use of the term "opportunity" may seem out of place, however, this term is being used by ISO 27001 in the context typically found in project management. In that context, a risk is a possibility that future events may not go exactly as planned or expected. Such deviations from the planned or expected path may have negative or positive implications for a project's success and the term "opportunity" is often used to describe deviations which would have a positive effect on the project outcome.

2.6.6.2 Information Security Risk Assessment

A previous version of the standard published in 2005 detailed a specific mandatory risk assessment process which involved identification of assets, threats, vulnerabilities, and the impact of any resultant breaches to the security requirements of assets. In the 2013 version of the standard this specific asset-based approach is no

longer mandatory, but a formal risk assessment is still required. The current version of ISO 27001 makes reference to the risk assessment methodologies of ISO 31000, however, the organization is free to determine which risk assessment methodology it deems appropriate to its own particular situation. The standard does require that risk owners are identified regardless of the method used to identify risks.

2.6.6.3 Information Security Risk Treatment

For those risks that are higher than the organization is willing to accept, the organization must identify ways to mitigate the risk either by reducing the probability of occurrence or reducing the impact of the occurrence or both. As described in the terminology section above, ISO 27001 refers to the methods of reducing probability or impact (or both) as controls. In the 2005 version of ISO 27001, the controls identified in Annex A of the standard were to be applied first and any remaining unaddressed risks could then be addressed using additional supplementary controls. In the 2013 version of ISO 27001 that sequence has been reversed so that the organization should first apply the controls which it may be obligated to use for contractual, regulatory, or other reasons. The controls listed in ISO 27001 Annex A are then used to supplement those controls which the organization has already deployed. This change reflects the fact that organizations may increasingly find themselves obligated to apply certain controls by a contract, trade group standards, or government regulation, or for other reasons.

ISO 27001 requires the explicit creation of a "statement of applicability" which details which controls have been implemented, why they have been implemented (in the case of controls which are not from Annex A.) or why controls from Annex A. have been omitted. The requirement to create this statement ensures that all of the controls in Annex A. must be considered by the organization and a justification for any implementation omissions of Annex A. controls must be recorded.

2.6.6.4 Information Security Objectives and Planning to Achieve Them

This section of the standard requires that an organization establish measurable and appropriate information security objectives at various levels in the organization. Such objectives must be communicated and updated as required and should include answers to the following:

- How the objective will be achieved?
- What resources are required?
- Who will be responsible?
- What is the timeline to completion?
- Which method will be used to evaluate the results?

2.6.7 Support

The support section of ISO 27001 calls on the organization to provide the necessary resources, skills, awareness, communications, and documentation to support the success of the ISMS.

2.6.7.1 Competence

The standard requires organizations to identify the necessary competences required to successfully operate the ISMS and to support the achievement of those competencies by the relevant roles through education, training, and experience.

The organization is required to measure its success in achieving this goal and is also required to document the necessary competencies and how they have been met by the organization.

2.6.7.2 Awareness

The standard requires the organization to make those working in the organization aware of the organization's information security policies, how their actions can contribute to the objectives of those policies and the implications (for the organization and the individual) of not conforming to the requirements of those policies.

2.6.7.3 Communication

Under this heading, the standard requires the organization to document the critical internal and external communication paths which can support the ISMS. This section should detail:

- The subject of the communications.
- The timing of the communications.
- The other party involved in the communications.
- Who will represent the organization in such communications.
- The process involved in such communications.

2.6.7.4 Documented Information

The standard requires the organization to create, update, and control such documentation as is required by the standard itself and such additional documentation as is necessary to ensure the effectiveness of the ISMS.

Under control of documentation, the standard makes specific reference to access, distribution, use, storage, preservation, change control, retention, and disposition as the areas to be addressed.

2.6.8 Operation

2.6.8.1 Operational Planning and Control

The organization is required to plan the processes necessary for the ISMS and to monitor their effectiveness.

2.6.8.2 Information Security Risk Assessment

The standard requires the organization to perform a risk assessment at planned intervals and when significant changes occur or are proposed. The organization is required to document and retain the results of such assessments.

2.6.8.3 Information Security Risk Treatment

The organization is required to implement the risk treatment plan and document the results thereof.

2.6.9 Performance Evaluation

2.6.9.1 Monitoring, Measurement, Analysis, and Evaluation

The organization is required to establish a system to monitor the effectiveness and performance of the ISMS.

2.6.9.2 Internal Audit

The standard requires the organization to "plan, establish and maintain" audit programs with the purpose of ensuring that the ISMS meets the organization's requirements and the requirements of the standard and that the ISMS is effectively implemented and maintained. The standard also requires that the results of such audits are reported to management.

2.6.9.3 Management Review

The management review required by the standard should consider internal and external changes which are relevant to the ISMS. The review should also monitor trends in areas such as nonconformance and should also consider audit results. The management review should consider feedback from interested parties, review the status and effectiveness of the risk assessment and risk treatment plan, and should review opportunities for continual improvement of the ISMS.

2.6.10 Improvement

2.6.10.1 Nonconformity and Corrective Action

The standard requires the organization to:

- React to nonconformities and their consequences.
- Document such nonconformities, the subsequent actions taken and the results of those actions.

2.6.10.2 Continual Improvement

The organization is required to continually improve the appropriateness and effectiveness of the ISMS as it relates to the organization's business objectives.

2.7 NIST Computer Security Resource Center

NIST's Information Technology Laboratory (ITL), has a broad mission to promote US innovation and industrial competitiveness by advancing measurement science, standards, and technology through research and development in information technology, mathematics, and statistics. The Computer Security Division (CSD) is a component of NIST's ITL that develops standards, guidelines, tests, and metrics that are designed to protect the cyber-infrastructure. The CSD's Computer Security Resource Center (CSRC) website[3] facilitates broad sharing of information security tools and practices. The CSRC also serves as a resource for information security standards and guidelines, and identifies key security web resources to support users. Between April 1991 and May 2015, the CSD has released 323 publications.

[3] http://csrc.nist.gov/.

Table 2.3 A selection of NIST cybersecurity-related publications

Publication number	Publication title	Publication date
800-12	An Introduction to Computer Security: the NIST Handbook	October 1, 1995
800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems	September 1, 1996
800-27 Rev. A	Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A	June 4, 2015
800-30 Rev. 1	Guide for Conducting Risk Assessments	September 12, 2015
800-34 Rev. 1	Contingency Planning Guide for Federal Information Systems	May 10, 2015
800-35	Guide to Information Technology Security Services	October 3, 2015
800-36	Guide to Selecting Information Technology Security Products	October 3, 2015
800-37 Rev. 1	Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach	February 10, 2015
800-39	Managing Information Security Risk: Organization, Mission, and Information System View	March 11, 2015
800-41 Rev. 1	Guidelines on Firewalls and Firewall Policy	September 9, 2015
800-44 Version 2	Guidelines on Securing Public Web Servers	September 7, 2015
800-45 Version 2	Guidelines on Electronic Mail Security	February 7, 2015
800-46 Rev. 1	Guide to Enterprise Telework and Remote Access Security	June 9, 2015
800-47	Security Guide for Interconnecting Information Technology Systems	August 2, 2015
800-50	Building an Information Technology Security Awareness and Training Program	October 3, 2015
800-60 Rev. 1	Guide for Mapping Types of Information and Information Systems to Security Categories	August 8, 2015
800-61 Rev. 2	Computer Security Incident Handling Guide	August 12, 2015
800-65 Rev. 1	Recommendations for Integrating Information Security into the Capital Planning and Investment Control Process	July 9, 2015
800-82 Rev. 2	Guide to Industrial Control Systems Security	May 15, 2015
800-83 Rev. 1	Guide to Malware Incident Prevention and Handling for Desktops and Laptops	July 13, 2015
800-92	Guide to Computer Security Log Management	September 6, 2015
800-94 Rev. 1	Guide to Intrusion Detection and Prevention Systems (IDPS)	July 12, 2015

(continued)

Table 2.3 (continued)

Publication number	Publication title	Publication date
800-100	Information Security Handbook: A Guide for Managers	October 6, 2015
800-114	User's Guide to Securing External Devices for Telework and Remote Access	November 7, 2015
800-122	Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)	April 10, 2015
800-128	Guide for Security-Focused Configuration Management of Information Systems	August 11, 2015
800-153	Guidelines for Securing Wireless Local Area Networks (WLANs)	February 12, 2015
800-160	Systems Security Engineering Guideline	May 12, 2014
800-161	Supply Chain Risk Management Practices for Federal Information Systems and Organizations	April 15, 2015
800-171	Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations	June 15, 2015

Many of these publications are first released in draft forms and then finalized based on comments. Some of the critical documents are also revised on an as-needed basis. The CSD's publications are broadly categorized in one of the following three categories:

1. Federal Information Processing Standards (FIPS) publications are issued by NIST after approval by the Secretary of Commerce pursuant to the Federal Information Security Management Act (FISMA) of 2002.
2. NIST Interagency or Internal Reports (NISTIRs) describe the research of a technical nature of interest to a specialized audience. The series includes interim or final reports on work performed by NIST for outside sponsors (both government and nongovernment). NISTIRs may also report results of NIST projects of transitory or limited interest, including those that will be published subsequently in a more comprehensive form.
3. Special Publications in the 800 series (established in 1990) are of general interest to the cybersecurity community.

This chapter discusses two key cybersecurity-related publications from NIST. Specifically, the Framework for Improving Critical Infrastructure Cybersecurity (NIST 2014) and the Special Publication 800-82—Guide to Industrial Control Systems Security (NIST 2015). In Table 2.3 we have listed a small selection of NIST publications which have particular relevance to the two aforementioned NIST publications. A comprehensive list of NIST CSRC publications including specialist

security information for specific technologies can be downloaded from http://csrc.nist.gov/publications/.

2.8 NIST Framework for Improving Critical Infrastructure Cybersecurity

The NIST Framework for Critical Infrastructure Cybersecurity (NIST 2014) was developed in response to Executive Order 13636 which called for the development of a voluntary risk-based cybersecurity framework. The authors of this framework have sought not to "reinvent the wheel," rather they provide an alternative process approach that is closely aligned to the typical requirements of critical infrastructure providers. The NIST framework makes many references to external resources such as the ISO/IEC 27000 family.

Perhaps the simplest way to contrast the NIST framework approach with that envisaged in ISO27001 is that ISO/IEC 27001 envisages a process cycle leading towards ISO/IEC 27001 certification followed by subsequent cycles during re-certification. The NIST framework by comparison encourages an organization to more rapidly complete a cycle and document their current status across multiple headings, even if the current cybersecurity posture is not where the organization ultimately wants to be. Once improvements have been made the new status can be compared with the old to document progress towards the desired security posture.

This is not to say that ISO/IEC 27001 could not be used in a similar way. By starting with a small scope and progressively increasing the scope through each iterative cycle, the ISO/IEC 27001 approach could result in similar progressive improvements in security posture. However, the NIST framework encourages organizations to consider the wider-scope initially, even if it will be some time before all of the identified issues can be addressed.

Ultimately, an organization which has iterated through the NIST framework and arrived at its desired security posture could then consider the ISO/IEC 27001 certification path. If the organization has been careful to align its NIST framework activities with ISO/IEC 27001 in areas such as risk analysis and application of controls then much of the NIST framework effort should be applicable to the ISO/IEC 27001 certification path.

2.8.1 Framework Core

The Framework Core is essentially a set of cybersecurity activities that are common across the critical infrastructure sectors. The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level.

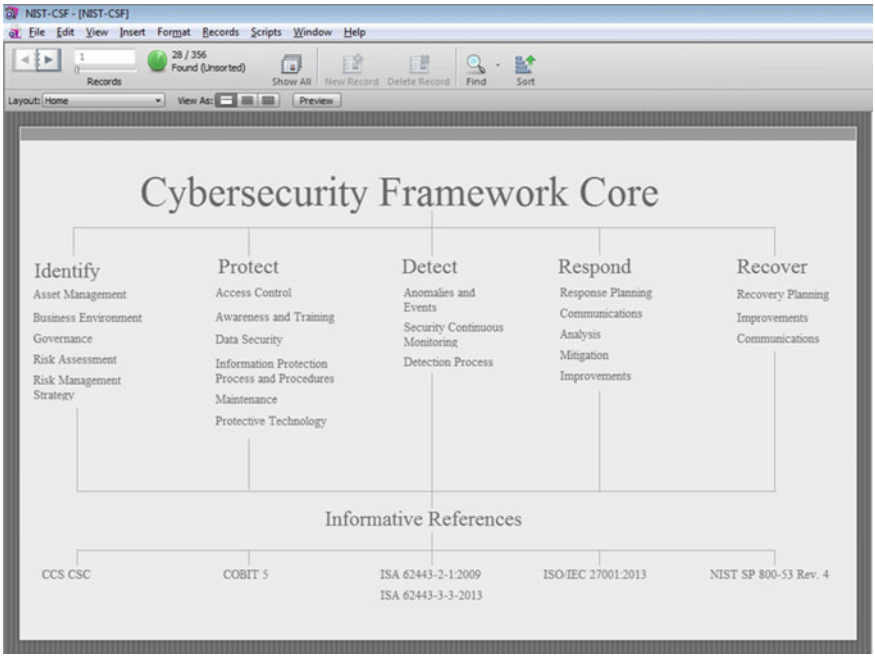


Fig. 2.2 NIST cybersecurity framework reference tool

2.8.1.1 Core Functions

The Framework consists of five core concurrent and continuous functions—Identify, Protect, Detect, Respond, Recover. When these functions are carried out, they provide a high-level strategic view of the lifecycle of an organization's management of cyber security risk. NIST has also developed a Cybersecurity Framework Reference Tool[4] which allows a user to browse the Framework Core by functions, categories, subcategories, informative references, search for specific words, and export the information. Figure 2.2 shows a screenshot of the reference tool.

The following sections contain an overview of the five core functions.

2.8.1.2 Identify

In order for an organization to improve its security posture, the organization must understand what it is attempting to protect. The identify function includes:

- Identification of assets and their security requirements.
- Identification of security threat sources.

[4] http://www.nist.gov/cyberframework/csf_reference_tool.cfm.

- Estimation of the probability that a threat source may breach an asset's security requirements.
- Estimation of the business impact or consequences of such breaches.
- Prioritization of the risks based on the estimated probabilities and impacts/consequences.
- Development of a risk management approach for the prioritized risks.

2.8.1.3 Protect

Having identified and prioritized the risks that the organization faces the organization will typically wish to apply additional protections as part of its risk management approach. The protect function reduces risks through application of controls such as:

- Policies
- Auditing of policy implementation
- User awareness training
- Access Controls
- Firewalls
- Encryption
- System patching and hardening

ISO27002 (ISO/IEC 2013a) and NIST 800-53 (NIST 2013) include comprehensive lists of such controls and in many critical infrastructure cases organizations will wish to use additional controls due to the nature of specific assets or the nature of the threats to which such assets are exposed.

2.8.1.4 Detect

While the controls that may be deployed under the Protect function above may be thought of as preventative controls, the controls which feature in the Detect function will typically be detective controls, which are concerned with the detection of a cybersecurity event.

The Detect function will typically include:

- Auditing activities.
- Logging and log analysis.
- Use of detective controls such as an Intrusion Detection System.

2.8.1.5 Respond

The Respond function covers how the organization responds to a cybersecurity event. The key purpose of this function is to encourage the organization to be

prepared for response by creating an incident response plan which will include a definition of key responsibilities and determine where they fall.

The Respond function will typically include:

- Creation and updating of an incident response plan.
- Identification of roles and responsibilities prior to, during, and following incident response.
- Post-incident review, analysis, and improvement processes.

2.8.1.6 Recover

The Recover function is concerned with the restoration of business operations.

The Recover function will typically include:

- Creation and updating of a business continuity plan.
- Creation and updating of a disaster recovery plan.
- Post-incident review, analysis, and improvement processes.

2.8.2 Framework Profile

An organization determines its target profile by selecting categories and subcategories from those provided in the framework based on its own business objectives and priorities. The target profile can then be compared with the organization's current profile to determine opportunities for improvement. As improvements in cyber security posture are implemented, the current profile will change and provide an indication of progress towards the chosen target profile.

2.8.3 Implementation Tiers

Implementation tiers reflect varying degrees of sophistication in cyber security management practices. The framework does not advocate that all organizations seek the most sophisticated tier; rather the framework indicates that an organization should select the tier that meets the organizations' objectives by reducing the risk associated with certain assets to a level acceptable to the organization. Thus, the implementation tiers should not be seen as representing maturity since the most sophisticated tier may not be appropriate to every organization.

The tiers are listed below along with a short description to indicate the level of sophistication of each tier. A full description of the tiers is available in the framework document (NIST 2014).

- Tier 1: Partial
  This is the least sophisticated of the tiers and describes low awareness and a somewhat ad hoc and reactive approach to cyber security.
- Tier 2: Risk informed
  In this tier, there is awareness of cyber security risk at the organizational level but the necessary structures to successfully manage cyber security across the organization are not in place.
- Tier 3: Repeatable
  In this tier, the organization has in place the structures to manage cyber security risk across the organization and the organization is able to respond to changes in risk.
- Tier 4: Adaptive
  This is the most sophisticated tier in which cyber security risk management is part of the organizational culture. Suitable cyber security risk management and improvement structures are in place and the organization fully communicates with external partners to achieve cyber security goals.

2.9 NIST Special Publication 800-82—Guide to Industrial Control Systems (ICS) Security

NIST 800-82 (NIST 2015) differs from both the ISO27001 and the cyber security described above in that it focuses directly on cyber security as it relates to ICS which is one of the most critical information asset of a critical infrastructure. NIST defines ICS to include Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC), while addressing their unique performance, reliability, and safety requirements. The ICSs are vital to the operation of the US critical infrastructures that are often highly interconnected and mutually dependent systems. It is estimated that approximately 90 % of the nation's critical infrastructures are privately owned and operated (NIST 2015).

To make this distinction clearer, consider a small gas, electricity, or water utility. Such a utility faces many cyber threats, but only a subset of these threats will be relevant to the ICS. Some threats, for instance, may relate to general customer data such as customer credit/debit card information. Such threats are broadly similar to the threats facing many retailers in terms of the nature of the threats and the impacts that they may cause. However, these utilities also face cyber threats which are quite different from those faced by general retail businesses, in that they target the control systems which are critical to the normal operation of the critical infrastructure. The potential impacts of such threats, when realized, can be vastly different from those faced by the non-critical business sector.

Historically, business and ICS networks were separate because the network topologies were vastly different. Even if a utility owner recognized the value of integrating ICS/SCADA data into their strategic decision support systems, they could not because of limitations in the network topologies. The SCADA systems relied heavily on serial connectivity and very low-frequency radio communications that could provide enhanced range and partial line-of-sight connectivity, none of which supported standard IP connectivity desired by business networks (Panguluri et al. 2011). Furthermore, many ICS components were in physically secured areas and the components were not connected to the traditional IT business networks or systems. However, the recent evolution in low-cost IP devices is promoting the replacement of the older proprietary solutions. This evolution also promotes the connectivity of corporate business systems and the ICSs provide remote access capabilities using industry standard computers, operating systems, and network protocols. While the new connectivity and integration supports new IT capabilities, it also increases the possibility of cyber security vulnerabilities and incidents.

By focusing on the ICS, NIST 800-82 is able to be significantly more specific in its recommendations than the other two standards discussed so far in this chapter. NIST 800-82's focus is broad enough to be relevant to all critical infrastructure entities which operate some type of ICS, yet narrow enough to be able to make specific recommendations relevant to the cyber security of typical ICS components and systems. NIST originally developed the SP 800-82 guidance to meet its statutory responsibilities under the FISMA and the Homeland Security Presidential Directive 7 (HSPD-7) of 2003. NIST SP 800-82 complements NIST SP 800-53's (NIST 2013) recommendations for security controls for Federal IT systems and organizations. NIST 800-82 is designed to specifically assist in developing and deploying an overall security program for ICS architecture including SCADA, DCS and supporting devices, such as PLCs, Remote Terminal Units RTUs, and intelligent electronic devices (IEDs). The standard document that is freely available includes the following five key sections:

- Overview of ICS
- ICS risk management and assessment
- ICS security program development and deployment
- ICS security architecture
- Applying security controls to ICS

Whereas confidentiality is often a particularly high priority requirement in many cyber security scenarios, the ICS security objectives typically follow the priority of availability and integrity, followed by confidentiality. Possible threat incidents that an ICS faces include the following: (NIST 2014)

- Blocked or delayed flow of information through ICS networks disrupting ICS operation
- Unauthorized changes to instructions, commands, or alarm thresholds, which could damage, disable, or shut down equipment, create environmental impacts, and/or endanger human life

- Inaccurate information sent to system operators, either to disguise unauthorized changes or to cause the operators to initiate inappropriate actions, which could have various negative effects
- ICS software or configuration settings modified, or ICS software infected with malware, which could have various negative effects
- Interference with the operation of equipment protection systems, which could endanger costly and difficult-to-replace equipment
- Interference with the operation of safety systems, which could endanger human life

At a minimum, the cybersecurity program implementation and measures at a critical infrastructure should address the following elements:

- Restrict physical and logical access to the ICS network, devices, and network activity.
- Implement measures to protect individual ICS components from exploitation.
- Restrict unauthorized modification of data.
- Implement measures to detect security events and incidents.
- Devise the ability to maintain infrastructure functionality during adverse conditions.
- Have a plan to restore the system after an adverse incident.

NIST SP 800-82 recommends that an effective cyber security program for an ICS should apply the "defense-in-depth," strategy by layering security mechanisms. The layering approach minimizes the impact of a failure in any one defense mechanism. A defense-in-depth strategy should include a variety of controls as described in the following sections.

2.9.1 Administrative or Directive Controls

- Performing a comprehensive risk assessment and developing a risk management plan.
- Developing security policies, procedures, training, and educational materials that apply specifically to the ICS. In addition, consider enhancing ICS policies and procedures based on the Homeland Security Advisory System Threat Level, deploying increasingly heightened security postures as the Threat Level increases.
- Addressing security throughout the lifecycle of the ICS from architecture design, to procurement, to installation, to maintenance, and to decommissioning.
- Restricting ICS user privileges to only those that are required to perform each person's job (i.e., establishing role-based access control and configuring each role based on the principle of least privilege).

2.9.2 Preventive Controls

- Implementing a network topology for the ICS that has multiple layers, with the most critical communications occurring in the most secure and reliable layer. Providing a logical separation between the corporate and ICS networks (e.g., stateful inspection firewall(s) between the networks, or unidirectional gateways). Employing a de-militarized zone (DMZ) network architecture (i.e., prevent direct traffic between the corporate and ICS networks). Disabling unused ports and services on ICS devices after testing to assure this will not impact ICS operation.
- Restricting physical access to the ICS network and devices.
- Employing reliable and secure network protocols and services were feasible.
- Applying security techniques such as encryption and/or cryptographic hashes to ICS data storage and communications were determined appropriate.
- Expeditiously deploying security patches after testing all patches under field conditions on a test-system if possible, before installation on the ICS.
- Using separate authentication mechanisms and credentials for users of the ICS network and the corporate network (i.e., ICS network accounts do not use corporate network user accounts).
- Using modern technology, such as smart cards for Personal Identity Verification (PIV).

2.9.3 Detective Controls

- Implementing security controls such as intrusion detection software, anti-virus software, and file integrity checking software, were technically feasible, to prevent, deter, detect, and mitigate the introduction, exposure, and propagation of malicious software to, within, and from the ICS.
- Tracking and monitoring audit trails on critical areas of the ICS.

2.9.4 Corrective Controls

- Ensuring that critical components are redundant and are on redundant networks. Designing critical systems for graceful degradation (fault tolerant) to prevent catastrophic cascading events.

NIST has also developed specific guidance on the application of the security controls in NIST Special Publication (SP) 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations to ICS. While many controls in Appendix F of NIST SP 800-53 are applicable to ICS as written, they may require ICS-specific interpretation and/or augmentation.

Table 2.4 Comparable control groups in NIST and ISO frameworks

NIST 800-53 control families	Examples of related ISO27002-2013 controls	
Name	Section	Title
Access control	11	Access control
Awareness and training	8.2.2	Information security awareness, education and training
Audit and accountability	15.3	Information systems audit considerations
Security assessment and authorization	15	Compliance
Configuration management	12.4	Security of systems files
Contingency planning	14	Business continuity management
Identification and authentication	11	Access control
Incident response	13	Information security incident management
Maintenance	12	Information systems acquisition, development and maintenance
Media protection	10.7	Media handling
Physical and environmental protection	9	Physical and environmental security
Planning	5	Security policy

2.10 Comparison of Controls

NIST 800-82 (NIST 2015) refers to the 18 control families defined in NIST 800-53 (NIST 2013). There is not a one-to-one mapping of the NIST 800-53 control families with the major control headings in ISO 27002; however, the two standards do cover much of the same ground.

By defining a range of common controls, these standards provide organizations with a template on which to build their own control framework. Note however that the standards also recognize that the changing nature of threats, vulnerabilities, and even assets means that organizations may have to supplement these common controls with new additional controls to address new forms of risk.

Larger organizations may wish to implement ISO 27001/27002 as their general information security framework but may also wish to use NIST 800-82 to address cyber security of their ICS. Despite the lack a one-to-one mapping between the controls in these different standards, it is possible to see distinct similarities in some areas. In Table 2.4, some examples are given of where ISO 27001 control headings cover similar ground to the corresponding NIST 800-53 control family. This list is not meant to be exhaustive, but gives some indication that by being aware of the two standards early in the process it would be possible for an organization to use NIST 800-82 for its ICS security within a larger ISO 27001/ISO 27002 framework without fully duplicating the efforts involved. NIST 800-53 revision 4 (NIST 2013) provides a table which gives an extensive mapping of ISO/IEC 27001 (ISO/IEC 2013b) controls with NIST 800-53 controls (NIST 2013).

2.11 Summary and Conclusions

For those charged with roles and responsibilities regarding an organization's cyber security posture, there are many resources available to assist. Many of these resources use a shared and increasingly standardized terminology and some familiarity with that terminology is beneficial.

Cyber security frameworks provide organizations with useful templates to guide their cyber security efforts. By leveraging the work which has already been done to develop these frameworks, an organization can achieve a better improvement in cyber security more rapidly than would otherwise be possible for a given resource expenditure. Frameworks are available in varying degrees of focus. They range from the broad applicability of ISO 27001/27002 through the critical infrastructure industry focus of the NIST Cybersecurity Framework for Critical Infrastructure to the ICS specificity of NIST 800-82. Each of these frameworks in turn references a wide range of additional documents and standards which can be drawn on by organizations. Where appropriate, organizations may wish to use elements from multiple frameworks to mold a structure that meets the specific requirements of their organization. Likewise, the controls advocated within the framework standards may be augmented as required by additional controls to meet new risks arising from changing threats, changing vulnerabilities, changing assets, changing business objectives, or other varying factors that may arise.

References

ISO, IEC. (2013a). *ISO/IEC27002:2013 Information technology—Code of practice for information security controls*. Geneva, Switzerland: ISO/IEC.

ISO, IEC. (2013b). *ISO/IEC 27001:2013 Information technology—Security techniques—Inormation security management systems—Requirements*. Geneva, Switzerland: ISO/IEC.

NIST. (2013). SP 800-53: Security and privacy controls for Federal Information Systems and Organizations. Washington, DC.

NIST. (2014). *Framework for improving critical infrastructure security*. Washington: DC, NIST.

NIST. (2015). *SP 800-82: Guide to Industrial Control Systems (ICS) Security*. Washington: DC, NIST.

Panguluri, S., Phillips, J. W. R., & Ellis, P. (2011). Cybersecurity: Protecting water and wastewater infrastructure. In S. Hakim, R. M. Clark, & A. Ostfeld (Eds.), *Handbook of water and wastewater systems protection* (pp. 285–318). Springer-Science: New York.

Chapter 3
Assessing Cyber Threats and Solutions for Municipalities

Scott J. White

Abstract Americans live, work, and play in cyberspace. However, our increasing reliance on cyber technologies makes us more vulnerable to those who would attack our digital infrastructure with the intent of undermining our security and economic prosperity. Vigilance, constant and unwavering, is the price all municipalities must pay to keep their cyber infrastructure safe from those who would use violence, or the threat of violence, theft, or vandalism to disrupt or destroy their cyber-systems. The threat is real. Cyber-attacks include the unintentional or unauthorized access, use, manipulation, interruption, or destruction of electronic information and/or the electronic and physical infrastructure used to process, communicate, and store that information. There have been numerous cyber-attacks in the last few years that have illuminated various vulnerabilities both in our computing hardware and software. These attacks have been target specific and sophisticated. A good cyber-attacker can disrupt the electronic controls of our power grids, water treatment plants, and telecommunications networks. As well, these cyber-criminals can interfere with the production and delivery of basic goods and services provided to us by our municipal governments. Ultimately, these criminals can undermine our privacy by stealing our personal information and creating false identities for profit. With a subject as critical as cyber security, there is no room for ambiguity in terms of what must be done. Municipalities must strengthen their capability to detect, deter, and defend against cyber-attacks. How municipalities respond in both theory and practice to threats from within its jurisdiction or beyond its borders, tests the validity and application of its security principles and strategies. This chapter will examine cyber security infrastructure and the threats facing municipalities; in addition, it will examine those mechanisms that once implemented, can create a more secure cyber infrastructure.

S.J. White (✉)
College of Professional Studies, The George Washington University, Enterprise Hall - B56, 44983 Knoll Square, Ashburn, VA 20147, USA
e-mail: sjw@drexel.edu

R.M. Clark and S. Hakim (eds.), *Cyber-Physical Security*,
Protecting Critical Infrastructure 3, DOI 10.1007/978-3-319-32824-9_3

Acronyms

BYOD	Bring Your Own Device
CPU	Central Processing Unit
DoS	Denial of Service
DDoS	Distribution Denial-of-Service
ICT	Information and Communication Technology
IP	Internet Protocol
ISIL	Islamic State of Iraq and the Levant
IT	Information Technology
NATO	North Atlantic Treaty Organization
SIGINT	Signals Intelligence

3.1 Introduction

Americans live, work, and play in cyberspace. However, our increasing reliance on cyber technologies makes us more vulnerable to those adversaries who would attack our digital infrastructure with the intent of undermining our security and our economic prosperity. Vigilance, constant and unwavering, is the price all municipalities must pay to keep their cyber infrastructure safe from those who would use violence, or the threat of violence, theft, or vandalism to disrupt or destroy their cyber infrastructure.

The threat is real. One only needs to be a casual observer of the nightly news to see the pervasiveness of cyber-attacks upon both, the private and public sector's Information and Communications Technology (ICT) infrastructure.[1] Whether it is the bulk theft of sensitive government employee information[2] or cyber-attacks against private retailers[3]; unlawful cyber intrusions are definitely on the rise, not only in the United States, but across the globe. These cyber-attacks would include the unintentional or unauthorized access, use, manipulation, interruption, or destruction of electronic information and/or the electronic and physical infrastructure used to process, communicate, and store that information.

[1]Information and Communications Technology (ICT): The acquisition, processing, storage and dissemination of vocal, pictorial, textual and numerical information by a combination of computing, telecommunication and video.

[2]Lisa Rein, *Largest employee union says hackers stole personal data on every federal worker*. Washington Post. June 11, 2015.

[3]*At least THREE more major U.S. retailers hit by cyber-attacks similar to the ones suffered by Target and Neiman Marcus, pundits say*. The Daily Mail. 13 January 2014.

The various cyber-attacks that have occurred worldwide in the last few years have demonstrated numerous vulnerabilities in both our computing hardware and software. And, as we have become blatantly aware, for the most part these attacks have been sophisticated and target specific.

A cyber-attack is not a benign occurrence, but rather these types of attacks have demonstrated that real harm can be caused, not only to the ICT infrastructure, but also to the operations of government and the economy. A skilled cyber-attacker can disrupt the electronic controls of our power grids, water treatment plants, and telecommunications networks, as well they can steal our confidential information and personal data for nefarious purposes.[4] In addition, these cyber-criminals can interfere with the production and delivery of basic goods and services provided to us by our various levels of government. And, it is important to note that our municipal governments, like those at the state and federal level, are not immune from a targeted cyber-attack. In fact, municipal governments may be more susceptible due to the fact that their defenses tend to be less robust than other branches of government. Ultimately, the danger lies in the fact that these criminal cyber-attackers can destroy our critical infrastructure or at the least undermine our privacy by stealing our personal information and creating false identities for profit.

In the physical world, we are conditioned from a very young age, to think in terms of security. When we are young, we are told not to talk to strangers or leave our processions unattended. As we get older, we are reminded to lock our homes and automobiles, especially if we are not going to be present. As we progress along life's highway, we find ourselves continually adapting to meet the needs of an ever changing threat environment. However, when it comes to ICT security, it is readily acknowledged that there is a lack of understanding between the user of the technology and potential cyber threats. People generally view physical security differently than they do cyber security. It is this gap in understanding the true nature of the threats, which leaves us all vulnerable to a targeted cyber-attack. An attack which can often be devastating in terms of the loss of crucial data, a reduction in operating efficiency or a complete loss of ICT assets.

With a subject as critical as cyber security, there is no room for ambiguity in terms of what must be done. Municipalities must strengthen their capacity to detect, deter, and defend against cyber-attacks. How municipalities respond in both theory and practice to threats from within its jurisdiction or beyond its borders, tests the validity and application of its security principles and strategies. How best to facilitate the prediction, prevention, containment, and response to cyber-criminal behavior is the challenge for municipal governments in our ever changing cyber

[4]Data is the electronic representation of information. It is the quantities, characters or symbols on which operations are informed by a computer, being stored and transmitted in the form of electric signals and recorded on recording media.

world. This chapter will examine cyber security infrastructure and the threats facing municipalities; in addition, it will examine those mechanisms that once implemented, can create a more secure cyber infrastructure.[5]

3.2 Cyberspace as Critical Infrastructure

Today, more than ever, we rely on ICT infrastructure. Advances in technology have led to great efficiency in the marketplace and as consumers; we have become more dependent on technology to make our lives easier and more productive. Various levels of government have also become increasingly dependent on ICT. The Federal Government alone now offers hundreds of commonly used services online, such as tax returns, social security forms, and student loan applications to name but a few. It is evident that our success in cyberspace is one of our greatest national assets. Protecting this success means, protecting cyber infrastructure against malicious misuse and other destructive attacks. This is a daunting task, because there is no simple way to detect, identify, and recover from attackers who cannot be seen or heard, who leave no physical evidence behind them, and who hide their tracks through a complex web of compromised networks and computers.

The world is both complex and interdependent. Critical infrastructures, which include cyber, have become linked in such a way as to promote efficiencies and operational effectiveness. Critical infrastructures rely on one another, albeit in varying degrees, to support the vast economy of the United States. Communications systems are now linked with IT[6] to create an ICT[7] environment that enables central monitoring and control over production and delivery processes across the breadth and width of the country and in some cases beyond. These advancements in ICT allow for greater connectivity of critical infrastructure, but it also links that infrastructure in such a way that has never been seen before. More importantly, this independency has left us vulnerable to those who would wish to use that technology contrary to the general good of the society. The challenge is to maintain the efficiencies and effectiveness of interdependent critical infrastructure whilst at the same time make that connectivity secure from malicious intrusion.

[5]Security mechanisms area class of security solutions rated in terms of security strength of protection and security assurance of implementation to address specific threats.

[6]Information Technology (IT) is the use of any computers, storage, networking and other physical devises infrastructure and processes to create, process, store, secure, and exchange all forms of electronic data.

[7]Information and Communications Technology (ICT) is a more extensive term and acknowledges the role of unified communications and the integrations of telecommunications.

3.3 Threats to the Physical Plant and Information Technology

A municipal government, like any other corporate enterprise, relies on information infrastructure to support their operational activities.[8] This interconnected information infrastructure is often subject to serious threats which by their very nature have the potential to adversely affect normal operations. These threats would include, but are not limited to, actual destruction, whether wanton or accidental, of the physical plant and/or the compromising of information, its integrity and its availability to be accessed and utilized.

3.3.1 The Physical Plant

The Physical Protection or Physical Security of ICT infrastructure is an important consideration for all municipal governments. The events of September 11, 2001 demonstrated how vulnerable we can be to a physical attack. When we consider physical protection, we tend to think of it in terms of the convergence of hazards and vulnerabilities. A hazard is simply a potentially damaging physical event, phenomenon, or human activity that may cause the loss of life or injury, property damage, social and economic disruption, or environmental degradation. When evaluating hazards, we are referring to the entire spectrum of hazards, whether they are natural or human-induced. Thus, there are a myriad of potential hazards that can align with vulnerabilities to cause irreparable harm to the physical plant.

To begin, let us discuss Natural Hazards. Natural hazards are a source of potential harm originating from a meteorological, environmental, geological, or biological event. These hazards would include, but are not limited to, tornadoes, hurricanes, floods, extreme weather, earthquakes, ice-storms, and infectious diseases. It is not difficult to find examples in our recent history whereby natural hazards have caused devastating consequences to both life and property. One only need to look at hurricanes Katrina (2005) and Sandy (2012) to understand how a single natural event can have long-term repercussions for both a community and a country.

Human-induced hazards on the other hand, are hazards that occur because of human action or error, whether malicious or unintentional, including technological failures. Both natural and human-induced hazards can have an adverse effect on the physical plant which could render it partially or fully inoperable.

In the end, security of the physical plant will require leaders to adopt a sound mitigation strategy. Mitigation as a general practice is performed in order to reduce

[8]An *Information System* is generally composed of data, computer platforms, communication networks, business applications, people and processes organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information.

either the likelihood of a hazard from manifesting as an actual event, or reducing the consequences of the hazard should an actual event occur.

Mitigation measures fall into two general categories, characterized by their dependence on physical modifications to the built or natural environments. These include: Structural Mitigation and Nonstructural Mitigation. The mitigation grouping that includes measures characterized as 'Structural' pertains to those measures that involve or dictate the necessity for some form of construction, engineering, or other mechanical changes or improvements aimed at reducing hazard risk likelihood or consequence. 'Non-Structural Mitigation', on the other hand, seeks to reduce the likelihood or consequence of risk through modifications in human action, human behavior, or natural processes. These mitigation strategies will be examined in greater length further in this chapter.

3.3.2 Information and Communication Technology

There are a myriad of ways in which adversaries can gain access to classified data in cyberspace. They can exploit vulnerabilities in either the computing software or the hardware and by doing so; can quickly gain access to valuable information. Two common techniques used by cyber-attackers are: first, the use of Malicious Software or Malware and second, the use of the Insider, (colloquially referred to as the Carbon Unit). Administrators working within municipal government must realize if they have not already, that it is no longer a question of whether their ICT infrastructure will be targeted; it is simply a question of when and how that breach will occur.

Malicious software or Malware is the most commonly used tool to gain access to a network. Malware is any software that gives partial to full control of a computer over to another computer. For example, it can be used to create an entry point into a network and once established, an adversary can gain information which can be used to execute specific cyber intrusions. Malware includes, but is not limited to: viruses, worms, Trojan Horses, Spyware, rootkits, and some forms of adware. The method most commonly used to transmit malware is common email. In this scenario, a computer operator opens an email or email attachment without properly scanning for potential threats, such as malware. Once opened, the malware begins to take over the key operating functions of the host computer.[9] Much of the time, the operator will not be aware that their computer has been hijacked until it is too late and the damage is done.

Malware sent via an email is the most common infiltration method of introducing malicious software to a computer, however, the greatest weakness to any cyber infrastructure is the carbon unit; the individual human operator; the insider. It

[9]Malware Defenses: Control the installation, spread and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering and corrective action.

is an unfortunate reality of today's workplace, that the employee must be viewed as a potential insider threat; a threat that must reluctantly be considered and guarded against by all employers. Simply, an insider is someone who can exploit their legitimate access to an organizations' computer infrastructure to engage in unauthorized activities. Such activities may include, but are not limited to: the disclosure of sensitive information; the facilitation of third-party access, the physical destruction of property, and the sabotaging of electronic or ICT assets.

Insiders pose a threat due to the fact that in the course of their day-to-day operations, they have access to key ICT infrastructure which is fundamental to the success of the enterprise. It is important to remember however, that not all insiders have the intent to cause harm. Often individual operators become unwitting participants to criminal conduct. Through poor judgment or a lack of knowledge, insiders can often be deceived into assisting an adversary in gaining access to a cyber infrastructure. Once again, this generally occurs when the computer operator opens an email or email attachment without adequately scanning for potential threats.

The insider with a criminal intent on the other hand, represents an immediate threat to the organization. Because of our dependency on computers and computer networks, a workplace environment has been created where employees, at all levels, have access to protected or classified information. As a result of this connectivity, it has become easier for insiders with criminal intent to gain access to sensitive information. Once access has been granted, the insider can corrupt, remove and/or circulate large amounts of data with relative ease. Perhaps the best example of the insider threat can be found in the WikiLeaks affair of 2010. In this case, it was alleged that an insider, Army Pfc. Bradley Manning leaked classified US diplomatic communiqués to WikiLeaks. In this case, Pfc. Manning was apprehended and later convicted of stealing and disseminating hundreds of thousands of pages of classified documents.[10]

Acknowledging the risks posed by the insider, employers still have the means at their disposal to lessening the threat to their organization by carrying out thorough pre-employment checks and by advocating a strong security culture. There will always be some degree of risk to the organization. However, if employers are going to maximize efficiency and create a robust customer focused enterprise; access to the ICT infrastructure is a requirement; thus, municipal governments will have to learn to work with some residual risk.[11]

Finally, many organizations regard personnel security as an issue resolved during the recruitment and application process. This is a flawed perspective. Security is a discipline that needs to be maintained throughout an employee's time

[10]US Army HHC, 2d BCT, 10th MTN Div (LI) (2010-07-05). "Charge Sheet of Bradley E. Manning" (PDF). Cryptome. Retrieved, 07/11/2015. US Army, MDW, OSJA, HQ CMD BN, USA (2011-03-01). "Charge Sheet of Bradley E. Manning (Additional)" (PDF). Cryptome. Retrieved, 07/11/2015.

[11]Residual risk—A risk that remains after security controls have been selected and implemented.

in service. This includes not just a robust pre-employment screening, but also; effective line management, clear policies, clear lines of communication, and a strong security culture. It should also include a formal process for managing an employee termination, whether through dismissal or voluntary separation.

3.4 Understanding External Adversaries in Cyberspace

Our computer infrastructure and the valuable information which is stored and disseminated through those systems have become an attractive target to an ever increasing group of adversaries. These adversaries could include foreign military and intelligence services, terrorist networks and criminals; both sophisticated and amateurish. These adversaries through their deliberate actions are illegally accessing computer networks, searching databases and causing systems to '*crash*' that is to say, stop functioning properly. Ultimately, these criminals are stealing our national security strategies and industrial secrets, as well as our personal information and identities. Theirs is often a silent crime. We do not always witness them, hear them, or apprehend them. Sometimes they do great harm to our ICT infrastructure, while other times they are more of a nuisance. In the end however, their actions are illegal and present a clear and present danger to government, to industry and to the country as a whole.

Acknowledging this, it is useful for security professionals to distinguish from those adversaries who are carrying out attacks for political or ideological purposes and those that may be perpetrating more traditional criminal conduct. By understanding the potential adversary, governments can institute the most appropriate strategies to defend against undesirable intrusions.

3.4.1 Foreign Governments: Intelligence and Military Services

While most of the publicly known cyber-attacks have been perpetrated by hackers or hacktivists, security authorities have long known that foreign governments have been acquiring, through the use of their security and intelligence services, gigabits of data on a daily basis.

The most sophisticated adversaries are those who work on behalf of foreign governments. Intelligence and military services of foreign states present the greatest challenge for those responsible for protecting our cyber infrastructure. In most cases, these intrusions are backed by well-resourced sovereign governments and lead by well-educated cyber-warriors. Their purpose is relatively simple; to gain political, economic, and military advantage over a targeted government, so as to have the capacity to disadvantage that government at some future time.

Global connectivity, which is facilitated by the Internet, gives foreign governments a powerful new method of conducting espionage and sabotage, whilst at the same time; these state actors can deny using their ICT infrastructure for nefarious means. In March of 2009, a group of Canadian researchers, working for the Information Warfare Monitor, revealed a network of over 1200 infected computers worldwide. They codenamed their investigation: '*GhostNet*'.[12] The infected computers represented several high-valued government targets, for example: the private offices of the Dalai Lama, the Indonesia's Ministry of Foreign Affairs and the Indian Embassy in Kuwait, as well as a dozen other sensitive computer systems linked to other governments around world. The researcher's report, which was published after a 10-month investigation, found three out of the four servers in the network were based in China, while a fourth was in the United States. According to the report, some of the IP (Internet Protocol) addresses used by the hackers were traced back to Hainan Island (China's Naval SIGINT), which is the location of the Chinese Governments signals and intelligence agency, better known as the Third Department of the General Staff, within the Department of the Central Military Commission.[13] A subsequent investigation further revealed the level in which computing infrastructures, including those of large international companies, were being exploited for cyber-espionage.[14]

Some foreign nation states, such as China, have declared publicly that cyber-attacks are a central element of their military strategy.[15] And, some of these states have been widely accused of using cyber-attacks to coincide with traditional military operations. These cyber-attack programs are typically designed to sabotage an adversary's ICT infrastructure; however, they also have the potential to affect medical emergency response systems as well. It is for these reasons that the United States and its allies understand that addressing cyber risks requires modernizing cyber-defenses and military doctrines. To this end, the North Atlantic Treaty Organization (NATO) has adopted several policy documents in regard to cyber defense.

Finally, it is generally accepted that, the resources necessary to develop and deploy sophisticated viruses and worms, against a government and its military; points directly to state involvement or state sponsorship. As a result, tracing the attack and identifying the originating entity is a difficult exercise and in the end may yield very little in terms of the understanding the adversary.

---

[12]JR02-2009, Tracking GhostNet: Investigating a Cyber-Espionage Network. Information Warfare Monitor. March 29, 2009.

[13]Ibid, p. 30.

[14]JR03-2010, Shadows in the Cloud: Investigating Cyber-Espionage 2.0. Joint report: Information Warfare Monitor & Shadowserver Foundation. April, 6, 2010.

[15]Shannon Tiezzi, *Chinese Military Declares the Internet an Ideological 'Battleground'*. The Diploma Magazine (Online Publication), May, 21, 2015.

3.4.2 Terrorism

At the outset, let us say, it is not the objective here to argue the nature of the word terrorism. We freely acknowledge the pejorative nature of the word. Seldom do terrorists identify themselves as such. Instead, they identify themselves as freedom fighters, members of liberation organizations or simply as the righteous. In addition, we must acknowledge that there is no universally excepted definition of terrorism. The word itself is a contested issue. When we read a newspaper or watch a television news report, most of us would tacitly agree that certain acts of violence are terrorism, but often we cannot agree on other actions. Ask any political scientist and they tell you that political and strategic concepts are difficult to define in a few words at the best of times. However, that does not mean to say that we cannot or should not use them. For example, there is no better alternative term, in our opinion, for the particular mode of violence which is indicated by the word terrorism.

The legal statute in the United States which defines international terrorism is, Title 18 USC Chapter 113B, S. 2331

> (1) the term "international terrorism" means activities that
>
> (A) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State;
>
> (B) appear to be intended - (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and
>
> (C) occur primarily outside the territorial jurisdiction of the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum[16];

Terrorism is asymmetrical warfare. And, cyber-attacks are the perfect asymmetric weapon, in that, unlike physical attacks, like those seen on September 11, 2001, a cyber-attack is relatively inexpensive to operationalize. In addition, it is often difficult, if not impossible, to identify those responsible. Cyberterrorism is any act that is aimed at undermining the social, economic, and political system of an adversary by destroying its digital infrastructure. According to the U.S. National Infrastructure Protection Center, cyberterrorism is defined as

> A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda.[17]

Terrorists and terrorist networks are moving quickly to incorporate cyber-operations into their strategic portfolios. We know for example that organizations

[16]Title 18 USC, Crimes and Criminal Procedure, Part I, Chapter, 113B, Terrorism, S. 2331.

[17]Dimitar Kostadinov, Cyberterrorism Defined (as distinct from Cybercrime), Infosec Institute. Retrieved, 07/10/2015. http://resources.infosecinstitute.com/cyberterrorism-distinct-from-cybercrime/.

such as the Islamic State of Iraq and the Levant (ISIL)[18] are using the internet to support recruitment, fundraising and propaganda campaigns. As well, terrorist organizations are acutely aware of the West's dependence on its cyber infrastructure. As such, they are relentlessly trolling cyberspace in hope of exploiting vulnerabilities in our security.

It is important to note that, although there has been demonstrated intent, on behalf of some terrorist groups to conduct a cyber-attack against the United States and its allies, these terrorists are yet to develop the technical capability to engage in such an attack. Acknowledging this, the US cannot become complacent; terrorist organizations are continually developing and acquiring new capabilities with the intent on launching a catastrophic cyber-attack against the West. Through the sharing of information and expertise in online forums, cyber-terrorists are increasing their knowledge and thereby, improving their chances at executing a successful cyber-attack.

3.4.3 Cybercrime

Where there is an opportunity for financial gain, there will always be those who will resort to criminal conduct to attain a perceived advantage. The criminal element has successfully expanded its operations into cyberspace. The most sophisticated among this element (Organized Crime) are utilizing the skills of cyber-attackers to engage in traditional criminal activities such as: identify theft leading to fraud, money laundering, and extortion via the cyber world.

The most common form of crime perpetrated against municipal governments is that of fraud. Simply, fraud is the deliberate act of deception, to secure unlawful gain or benefit. Cyber-criminals regularly use false or stolen credentials (social security numbers, drivers licenses, birth certificates, etc.,), to engage in some form of fraud against public entities. The difficulty for municipal governments is, as they continue to migrate more of their services each and every day to an online platform; the cyber-criminal will continually seek opportunities to exploit that resource.

In some cases however, the sophisticated cyber-criminal does not want to defraud from government, but rather, they just want to use the government's own ICT infrastructure as a platform to engage in other criminal activities, such as sending spam or phishing emails. It is not uncommon to have organized crime '*piggyback*' a legitimate computer network to engage in nefarious activities.

[18]Also known as ISIS, the Islamic State of Iraq and Syria or the Islamic State of Iraq and ash-Sham.

3.4.4 Hacking and Hacktisivism

Hacking remains a challenge for all levels of government. Granted, most incidences of hacking can be attributed to criminal behavior, however, there is a growing movement toward activists targeting computer networks in an attempt to target critical infrastructure. This new breed of '*tech savvy*' activist is colloquially referred to as a 'hacktivist'. Acting within a group or alone, these individuals have moved from street protesting and vandalism to the cyber world.

Hacktivists seek notoriety. For these individuals' success comes in the form of disrupting websites and other forms of social media. The embarrassing of, or causing nuisance to, the reputation of a government or other enterprise is their goal.

There are two techniques of choice for the majority of Hacktivists: the Denial-of-Service (DoS) attack and the Distributed Denial-of-Service (DDoS) attack. A Denial-of-Service (DoS) attack involves a malicious attempt to disrupt the operations of a computer system or network that is connected to the Internet. The most common form of attack is one which disrupts the operations of the computer system or network by consuming the bandwidth of the victim's network or overloading the computational resources of the victim's system.[19]

A DDoS attack occurs when a system, service, or network is overwhelmed with so much traffic from multiple sources that it becomes unavailable. In this scenario, an adversary builds a network of infected computers, known as '*botnets*', by spreading malicious software through emails, websites, and other forms of social media. Once infected, these computers can be controlled remotely, without their owners' knowledge and attack a target at will. A cascade of traffic, generated by the '*botnet*,' quickly overwhelms the targeted computer system causing it to go offline. Hacktivists utilize DDoS attacks, because they are relatively inexpensive and easy to construct; more importantly though, the DDoS attack works exceedingly well at silencing the target.

Perhaps two of the most infamous DDoS attacks, perpetrated against sovereign governments, were those launched against Estonia in 2007[20] and in Georgia in 2014.[21] These attacks demonstrated how effective the DDoS technique is at disabling a target. Government websites, internet traffic, banks, the media, and mobile communications were all adversely affected by these attacks. The scale of the attacks and the ongoing political tensions between Russia and its neighbors, pointed an accusatory finger toward Moscow, however, formal blame for the attacks, could not be determined definitively.

---

[19]The most common form of defense against a DoS attack is to locate the source of the attack and to filter out the attacker's network traffic from that source.

[20]Ian Traynor, *Russia accused of unleashing cyberwar to disable Estonia.* The Guardian, Wednesday 16 May 2007.

[21]Tom Fox-Brewster, '*State sponsored*' *Russian hacker group linked to cyber attacks on neighbours*. The Guardian, Wednesday 29 October 2014.

Countering a DDoS attack can be very difficult. The attacker is ultimately seeking to saturate a finite resource of the victim, be it bandwidth, CPU cycles or disk space. The defender on the other hand, is seeking to provide sufficient resources, or to stop a sufficient amount of the attacker's messages, so as to prevent that saturation. A determined DDoS attack is difficult to mitigate fore, however, websites can be protected by hosting cached content across many servers; but it is important to note that, this solution can be very expensive and thus, cost prohibitive for municipalities.

Finally, in 2011, the Hacktivist group, Anonymous announced that it had replicated the code for the Stuxnet virus which was responsible for sabotaging the uranium enrichment facility at Natanz, Iran. Anonymous is a loosely affiliated group of international Hacktivists who are gaining in popularity as a result of their actions and all indications are that they will only increase their attacks in the coming years. Following the 2015 terrorist attacks in Paris, Anonymous declared war on ISIL and in a video released to world, vowed to disable Twitter accounts of those link to the terrorist organization.

Malicious hacking by hacktivists who target classified data or critical infrastructure must be viewed through the lens of national security, thus hacktivists cannot be seen as benign hackers motivated by protected or technical challenges, but rather as real threats to a nation security.

3.5 How Can Municipal Governments Respond?

So, now that we have established a fair amount of "*doom and gloom*" the question is; how can municipal governments respond, not just in theory, but in practice? The United States is probably the most internet dependent nation in the world. And, although it may appear that its adversaries have the upper-hand; there are many things governments, including municipal governments, can do to protect themselves from malicious intrusions into their cyber infrastructure. These responds would include, but are not limited to: (1) establishing an ICT Risk Management System and corresponding policies; (2) introducing Network Security Protocols; (3) implementing an Education and Awareness program; (4) monitoring for Malicious Software or Malware; (5) establishing rules for Remote Working and Private Devises; (6) delineating User Privileges and (7) developing Private, Public Partnerships.

3.5.1 ICT Risk Management System

All ICT departments should establish a rigorous and robust ICT risk management system. An essential part of cyber security is defining the risk strategy and acceptable levels of risk in such a way that they are aligned with the needs of the municipal government's operations. The purpose of risk, threat, and vulnerability

assessments are to provide decision-makers with a clear picture of key undesirable events (current and potential), and the probability of those events occurring, their possible repercussions, and recommendations to minimize or mitigate for specific risks, threats and/or vulnerabilities.[22]

Once risk to the ICT infrastructure has been accessed; municipal governments must then establish ICT security policies to mitigate or eliminate altogether potential risk. An ICT security policy is simply a set of mechanisms by means of which information security objectives can be defined and attained. For ICT security there are three key objectives: *confidentiality, integrity,* and *availability*. Simply, the information must be only available to those who are authorized to view it (confidentiality); protected from unauthorized modification (integrity) and readily obtainable when it is needed (availability).

3.5.2 Network Security

Connectivity is both a necessity and vulnerability. When municipal governments connect to untrusted networks, such as the Internet, they have the potential to expose their organizations to malicious intrusions. To prevent these occurrences, governments must follow industry standards when designing and configuring their systems. All networks and network devices must be configured to a secure baseline. That means, that all traffic through the network must be filter so that only that traffic required to support the municipal government's mission is allowed.

There are a variety of standards; however, the IT industry tends to view the ISO/IEC 27001:2013—Information technology—Security techniques—Information security management systems—Requirements, as the baseline for IT (ICT) security. Acknowledging this, in February of 2013, President Obama issued Executive Order 13636, entitled, *Improving Critical Infrastructure Cybersecurity*. EO 13636, focused primarily on information sharing and the development of a cyber security framework for critical infrastructure. It defined a framework and a set of standards, methodologies, procedures, and processes that critical infrastructure owners and operators could use to reduce their cyber risks.[23] Although, the Executive Order emphasized large critical infrastructure connectivity, there is nevertheless much that can be used in terms of framework analysis by municipal governments.

Municipal governments must design and implement ICT security policies which conform to industry best practices and standards. And, these policies must be adhered to by all employees, regardless of their position within the organization.

---

[22]ICT Risk Management is the process by which organizations manage ICT security risks. ICT risk management is achieved through ICT security and other risk management processes.

[23]Department of Homeland Security, Integrated Task Force, Executive Order 13636: Improving Critical Infrastructure Cybersecurity. (Incentives Study Analytic Report). DHS, Washington, DC, June 12, 2013.

3.5.3 Education and Awareness

Awareness campaigns emphasizing the lessons learned through education and training can assist greatly in keeping employees aware of their obligation to remain vigilant against becoming a victim of a cyber-attack. A municipal government cannot expect all of its employees to have the technical knowledge base of their adversaries; however, understanding the potential threats and vulnerabilities can go a long way in protecting their ICT infrastructure from an attack. The implementation of ICT security policies is the first step in securing the infrastructure. The second step is to educate employees as to their obligations and responsibilities in reference to those policies. The easiest way to acknowledge this is, to have the ICT security policies be incorporated into the 'terms and conditions' of employment.

While clearly defined roles and responsibilities are important in achieving cyber security, Government's success in securing its ICT infrastructure is largely dependent on its employees; therefore municipal governments must make education and awareness an integral part their business model.

3.5.4 Malicious Software or Malware

Enhancing the resilience of the ICT infrastructure can be achieved through the appropriate combination of security measures to address the intentional or unintentional exposure to malicious software or malware. Municipal governments should introduce policies which directly address the enterprise processes. Such processes would include email, web browsing, and personally owned devises which are vulnerable to malware. As well, ICT security personal should continuously scan for malware using the most up-to-date antivirus programs. All information, supplied to, or emanating from the governments ICT infrastructure must be scanned for malicious content.

3.5.5 Remote Work (Telecommuting) and Private Devises

Modern offices have seen radical changes in just a few short years. Today, employers are increasingly likely to support their operations with mobile technology. Many of these devises might not have existed five years ago. As such, new and exciting ways of working have evolved very rapidly and while this can bring many benefits to both the employer and employee, there are also tremendous risks to the ICT infrastructure that need to be appropriately managed.

Allowing employees to work from home and use their own devises has become increasing popular in today culture. With the rapid increase in the use of mobile devices and the growth of remote and flexible working; employees now expect to use their own laptops, phones, and tablets to conduct business.

Personally owned devices are designed to facilitate the easy (and often automatic) sharing of data, and device owners routinely share personal information with other users especially in the Cloud.[24] Bring Your Own Devices; (BYOD) policy should highlight the risks of sharing business data with unauthorized users. Governments must consider how security problems in personal applications (e.g., blogs, social media) may affect the organization's applications, information, and network services.

3.5.6 User Privileges

One way of limiting access to various parts of a network is by user privileges. Users should only be provided those privileges required to perform the duties as prescribed in their job description. ICT security managers should limit the number of privileged accounts for such essentials roles as, systems or database administrators. Monitoring user activity, especially sensitive information and privileged account actions, (i.e., creating new accounts, changing passwords, etc.,), should be part of the day-to-day operations of the ICT management group.

3.5.7 Private, Public Partnerships

Threats to the government are not unique. Given the rapid changes in ICT, it is apparent to most that the existing defenses will be insufficient to truly protect ICT infrastructure from being corrupted or destroyed by a determined adversary. In light of the interconnectivity of all critical infrastructures,[25] private–public partnerships are a necessity. Partnerships are required amongst governments, law enforcement, the research and development community, and private industry. In this scenario, all stakeholders can work to manage risks, reduce vulnerabilities, and strengthen the resilience of the ICT infrastructure.

3.6 Conclusion

The threat of cyber-attacks is continually evolving and there is no doubt that the frequency and severity of malicious intrusions are accelerating at an alarm pace. Protecting any municipal governments ICT infrastructure and data will remain a

[24]Cloud computing is the sharing of computer applications, software, infrastructure and services over the internet by a third-party service provider.

[25]John D. Moteff, Critical Infrastructures: Background, Policy and Implementation. Congressional Research Services, CRS Report, June, 10, 2015.

constant and evolving challenge for individuals tasked with the responsibility of keeping those infrastructures secure. Sharing our collective knowledge, working to build private and public partnerships, implementing new initiatives, and remaining ever vigilant against those adversaries who wish to do us harm; these are our obligations and our responsibilities.

Chapter 4
Cyber Perimeters for Critical Infrastructures

A.F. Ginter

Abstract Modern businesses use industrial control system networks to control the physical processes essential to water treatment and distribution systems, electric generation, transmission, and distribution systems, manufacturing systems, as well as petrochemical pipelines and many other industrial processes. Today, control system networks employ conventional computing hardware and software products extensively, but the similarity between control systems and Information Technology (IT) systems is deceiving. The application of standard IT cyber security best practices to control systems yields singularly vulnerable control system networks. This chapter reviews high-level differences between IT and control system networks, and applies these differences to the task of securing the cyber perimeter of industrial control system networks. Safety, reliability, and cyber-sabotage-prevention imperatives are leading to an evolution of control network perimeters away from porous IT-style firewalls, in favor of hardware-enforced unidirectional gateways. This chapter examines the history and evolution of perimeter protection for control system networks, modern threats and attacks, the limitations of IT-centric protections, and the unidirectional protections being deployed increasingly at all types of industrial sites.

4.1 Introduction

Industrial control systems are the computers and networks that control large and sometimes dangerous physical processes, including the electric grid, water treatment systems, petrochemical pipelines, and many others. Many of these industrial processes are classed as "critical national infrastructures" by governments and regulatory bodies, because of the degree to which modern societies depend on these physical processes. Especially in large modern urban centers, the standard of living for the vast majority of people depends critically upon reliable access to electricity,

A.F. Ginter (✉)
Waterfall Security Solutions, Calgary, Alberta, Canada
e-mail: andrew.ginter@waterfall-security.com

R.M. Clark and S. Hakim (eds.), *Cyber-Physical Security*,
Protecting Critical Infrastructure 3, DOI 10.1007/978-3-319-32824-9_4

clean drinking water, sewage treatment, and fuel to permit the transport of foodstuff and other goods to these large, dense populations. Any sustained interruption to these critical industries puts large population centers at risk.

In addition, most large industrial processes are intrinsically dangerous. The more powerful a tool is, the more useful that tool is as a weapon. Large power plants, water treatment systems, refineries and other industrial sites are very powerful tools, and elements of the physical processes at these sites pose safety risks to workers at the site and to residents of nearby communities. Coal-fired power plants for example, generally contain large reservoirs of toxic ammonia to scrub acid-raid-causing compounds out of the products of combustion. Water treatment plants use large amounts of chlorine, which is toxic in high concentrations. Refineries heat large amounts of volatile petrochemicals to high temperatures in distillation towers and catalytic crackers.

At all of these sites, cyber security is generally not an end in itself, but rather is part of the site's safety program. The first priority for cyber security at the vast majority of industrial sites is protecting worker safety, environmental safety, and public safety. The second priority is reliability—to keep the billion dollar investment that is the physical, industrial process working.

How is the cyber security of industrial sites assured? In a sense, all cyber security starts at a site's physical and network perimeters. If any network of computers transitions from a "normal" state to a "compromised" state, that compromise had to arrive from somewhere; it somehow had to enter the network. Control system equipments might be compromised by messages from an outside network, by attack code carried into the site on removable media, by compromised equipment being carried into the site, or by people. Insider attacks can only occur if insiders physically cross a security perimeter and carry out their mis-configuration, mis-operation or other attack. Thus, cyber perimeters define every site's potential attack vectors.

4.2 History of Control System/Corporate Network Integration

Historically, the industrial cyber security problem was simpler than today, because industrial networks were "air gapped". The term "air gap" comes from the days before ubiquitous wireless communications. In that era, an "air gap" meant that no online connection of any sort existed between the industrial network and any public network, such as the Internet or the phone system, however indirect that connection might be. The safety and reliability of the control systems operating these large industrial sites were therefore safe from online, remote compromise. To compromise an air-gapped site, an attacker needed to either physically gain access to the site, or compromise or deceive a legitimate employee, contractor or visitor into carrying out the attack, or carrying the attack into the site.

Air gaps started disappearing in large numbers in the mid-1990s. This was the beginning of what the Gartner Group coined "IT/OT integration"—a term which has since been adopted widely. As control system networks increasingly used the same computers, operating systems, software, and networking components as information technology (IT) networks, separate IT and operations technology (OT) organizations made less and less sense. As a result, IT and OT organizations today often report to the same C-level executive, often share personnel and skill-sets, and sometimes use common processes for purchasing, maintenance, software license management, network and security monitoring and cyber security incident response.

More troubling, the integration of IT and OT teams and processes was and is almost universally associated with increased interconnection of IT and control-system networks. Since the mid 1990s, one industry after another has discovered the benefits of using control system data as part of business decision processes.

For example, when corporate computer systems are able to understand exactly how long and how hard each costly piece of industrial equipment has been used, those systems can delay maintenance. This "predictive maintenance" function delays costly equipment maintenance if industrial equipment was not used at 100 % of its capacity for the entire period since the previous scheduled maintenance. Out of the high-level applications, driving IT/OT network integration, predictive maintenance alone claims to reduce operating costs at large industrial sites by 3–7 %. At some sites, this is the site's entire operating profit margin. Many other high-level examples exist, including real-time access to materials and product quality measurements, make-to-order manufacturing and real-time adjustments in manufacturing schedules to win sales.

All of these profitable information-sharing applications provide compelling business motivations for integrating IT and OT networks. The problem with IT/OT network integration, as opposed to IT/OT team integration or business process integration, is that network integration introduces new cyber security risks. In the absence of any cyber security protections, attackers could simply connect to corporate networks through the Internet, reach through those corporate networks into industrial networks, and mis-operate the large, powerful equipment at an industrial site. This was and is a completely unacceptable risk to safety, to equipment at the site, and to reliable operations.

4.3 Traditional Network Perimeter Security

Since the early 2000s, cyber security best practices, guidelines, standards, and regulations have emerged to address this risk. For roughly a decade, nearly all such advice for protecting the IT/OT interface used firewalls as the foundation of cyber-perimeter protections. Since about 2010, this advice has been changing, largely because of fundamental limitations as to the security protections that

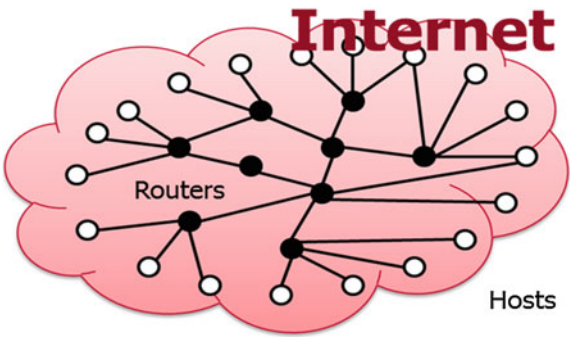


Fig. 4.1 The Internet

firewalls are able to provide to industrial networks. To understand these limitations, let's look at a very high level at the nature of modern industrial control system networks, and modern firewalls.

Essentially, all modern control-system networks use the Internet Protocol (IP) to some extent, and most control networks make extensive use of IP communications. A simplified model of the Internet is illustrated in Fig. 4.1.

The Internet can be thought of as a set of hosts, routers and communications links, all exchanging Internet Protocol (IP) packets. In Fig. 4.1, hosts create IP packets and send those packets to other hosts. In other words, hosts are the end-points of almost all IP communications. Routers forward packets. Routers find a path or "route" through the "twisty maze of connections" for each IP packet, so that each packet can be transmitted through that route to the host that is the packet's destination. In practice, the modern Internet consists of additional components, including switches, bridges, gateways, and other more exotic elements, but the simplified model of Fig. 4.1 is enough to understand the cyber-perimeter security risks of industrial control systems, as well as how those risks can be addressed.

Traditional IT security guidance recommends deploying firewalls when one network should be protected from attacks originating on another, less-trusted network. In the terminology of Fig. 4.1, a firewall is a router with a filter. The filter examines every packet passing through the firewall and asks if that packet matches any of the rules in the firewall's configuration settings. If the packet matches a rule, the firewall forwards the packet to whichever communications link the router component has calculated is the correct link for the packet. If the packet fails the firewall filter's test, the firewall generally discards the packet.

Modern firewalls include this basic packet-filtering capability, and generally include a whole host of additional features, including:

- Virtual Private Networks (VPN): encrypted connections to permit remote users to access equipment on a firewall-protected network,
- Intrusion detection systems (IDS): compare each packet against criteria attempting to determine whether each packet constitutes an "attack" in some sense of the word, and report "bad" packets,

- Intrusion prevention systems (IPS): make intrusion detection capabilities part of the firewall filter, in order to drop packets that the intrusion detection system has flagged as attacks,
- Stateful inspection: maintain state information about Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) dialogs in progress to augment decision-making in the firewall filter,
- Deep packet inspection: examine application payloads in IP packets and allows filters to express allowed/not-allowed rules in terms of application concepts, for example: "allowed to update facebook, but not to post a picture,"
- Inline anti-virus scanners: examine files passing through the firewall for matches on anti-virus signatures, and
- Firewall-based accounts and passwords: require users to log into firewalls in order to enable communications from those authenticated users' computers through the firewall.

In spite of this impressive-sounding list of features, many security issues accompany modern firewalls. Fundamentally, no firewall filter is, or can ever be, perfect at distinguishing "good" packets from "attack" packets. Worse, all firewalls are software. The problem with software is that all software has defects. Some defects are security flaws, and so in practice, all software can be hacked, even firewall software. To see evidence of this, simply visit any professional-class[1] firewall vendor's website, and see how many security updates have been issued for that vendor's firewalls in the last month.

Traditional IT security advice as applied to industrial control system perimeters contains many rules and recommendations that try to address these fundamental limitations of firewalls to at least some degree. More modern control-system security standards, regulations and guidance are evolving away from recommending firewalls at the perimeter of the most important control system networks, and towards recommending unidirectional security gateways.

Each of these topics is addressed below.

4.4 Limitations of Firewalls

Common wisdom holds that "if I have a firewall, and encryption, then I must be safe." This is, unfortunately, far from the truth. Nothing is ever absolutely safe, reliable, or secure. Each of safety, reliability and security are a continuum; we can always be more secure, or less secure. This means that every defensive posture, no matter how sophisticated, can be compromised. Let's look at some of the ways attackers compromise firewalls and the industrial control systems behind those firewalls.

[1]Note that vendors of consumer firewalls often do not publish security updates for their equipment's firmware, in spite of the security flaws that are routinely discovered in such firewalls.

4.4.1 Phishing and Watering-Hole Attacks

The most common way to breach a firewall is to deceive an insider at a targeted organization into using their computer to pull an attack through the firewall:

- "Phishing" pulls attacks through email systems. The attacker crafts email that tries to deceive a victim into either opening a compromised attachment, or visiting a compromised website. The website may try to deceive the victim into downloading attacks or malware, or to deceive the victim into providing a user name and password to the site.
- Watering-hole attacks compromise a website and try to deceive either the victim or the victim's browser into downloading malware.

Firewall vendors do what they can to design firewalls to detect and block these attacks, but no such measures are perfect. Most mail servers, even firewall-protected servers, accumulate some number of phishing emails every year. Most browsers attempt to download malware on a regular basis. Encrypted communications are often thought of as a means of addressing some firewall vulnerabilities, but encryption provides no protection at all from phishing attacks. As a rule, this class of attack is pulled right through encrypted connections to electronic mail servers and compromised websites. Encryption is designed to provide protection against so-called "man in the middle" attacks. When an endpoint of encryption is compromised, such as a mail server containing attacks, or a website containing attacks, encryption provides no protection at all.

4.4.2 Stealing Passwords

The easiest way to break through a firewall is to steal a password. This might be accomplished simply by turning someone's keyboard over and looking for a sticky note with a password written on it. Or sometimes an attacker can simply pick up the phone and call a firewall administrator, weave a convincing tale of woe, and politely ask for a password. Sometimes technology is involved, such as keystroke loggers that record all keystrokes entered into a computer. Attackers then review this record to see which of the keystrokes are entered in contexts that suggest they are passwords.

With an account password in hand, attackers can connect through firewalls and log into industrial systems. With the firewall administrator's password in hand, attackers can simply log into the firewall and reconfigure the device to permit access to protected networks.

4.4.3 Compromising Trusted, External Systems

In a world of integrated IT and OT networks, computers on OT/industrial networks are frequently configured to trust computers on IT/corporate networks, through firewalls. Compromising a trusted IT computer can then provide an avenue to attack OT computers.

For example, many OT networks are configured to trust Active Directory (AD) controllers on IT networks. AD controllers manage accounts and passwords. With a central AD controller deployed, IT staff can, with one simple user interface, modify permissions or even disable accounts for all personnel, company-wide, on all equipment, company-wide. If an employee leaves the company for example, disabling their account in the AD controller disables the account in all equipment that trusts the controller.

But this trust relationship also turns the AD controller into a single point of compromise for every machine in the company, including control-system equipment. If an attacker can guess a password or otherwise gain control of a domain network-administrator account, that attacker can instruct the Active Directory controller to create new administrator accounts and passwords on all equipment, company-wide. The attacker can now use those accounts to log into any industrial equipment that exposes a login prompt through a firewall.

4.4.4 Forwarding Attack Packets

Firewalls forward messages. In order for most IT systems to retrieve data from an industrial server, the IT system must send a request to the firewall-protected industrial server, and the industrial server responds with the requested data. If an attacker has taken over a machine or an account on an IT network that is permitted to send queries to an industrial server though, that machine or account can be used to launch attack packets at the industrial server through the firewall. The firewall filter will consider each such message and response, and will forward any legitimate packets or attack packets that pass the filter criteria. Since no firewall filter is perfect, some kinds of attack messages will always pass through the firewall into the supposedly-protected industrial server.

4.4.5 Attack through a VPN

Virtual private networks (VPNs) are software that encrypts packets across less-trusted networks such as the Internet. These packets are generally decrypted again by a VPN-aware firewall at the destination of the connection. The purpose of the VPN software on a remote computer or laptop is to provide that computer and

user the illusion that they are directly connected to a distant, private network. When a VPN connection is active, remote users can access corporate or industrial network resources as easily as they could access those resources when the laptop or computer was physically at the site on the other end of the VPN connection.

The problem is that malware accesses resources as well. Businesses may think they are giving a VPN password to permit a trusted employee to connect to a secure network, such as an industrial control network. In fact, when a trusted employee provides a VPN password to the VPN software on a remote laptop, it is not the user who is remotely connected to the trusted network, but the laptop. Malware resident on the VPN user's laptop can generally attack the destination network right through the VPN connection. VPN's generally encrypt attack packets just as effectively as they encrypt benign packets.

4.4.6 Firewall Vulnerabilities

All firewalls are software, and all software has vulnerabilities. Some of these vulnerabilities are well known to both attackers and defenders, because the firewall vendor has announced the vulnerability and provided a security update to address the vulnerability. It is imperative that such updates be installed promptly on all firewalls in an organization, lest attackers use the now-public information about the vulnerability to defeat un-updated firewalls. Other vulnerabilities are discovered by attackers and are exploited by those attackers, without telling anyone. There is little any site can do to prevent the latter attacks from reaching through firewalls.

4.4.7 Errors and Omissions

Modern, professional-grade firewalls are complex. The smallest configuration error can lead to incorrect connectivity with protected networks. In the worst case, configuration errors can disable all firewall filtering for some or all IP addresses, effectively turning the firewall into a simple router.

4.4.8 Forged IP Addresses

Most firewall rules are expressed in terms of IP addresses—for example, "allow this set of IP addresses to send TCP/IP packets to that port on this other IP address." If an attacker can issue packets containing a trusted IP address, those packets are likely to be routed right through the firewall to attack protected equipment.

For example, if a manager leaves the office with her laptop in hand, that laptop's IP address is no longer used on the office network. Another employee in the office

can now use his own computer's operating system control panel to change the IP address on the computer. With this done, his computer acquires all of the permissions to route packets through the firewall that the firewall filter has assigned to the manager's IP address.

4.4.9 Bypass the Firewall

If a route can be found from an attacking network to a target network, and that route does not pass through a firewall deployed to protect the target network, that firewall never sees the attack packets. One common way this happens is with rogue wireless routers; well-meaning employees install wireless routers on critical networks in the name of "increased productivity" without considering security consequences. Another route around firewalls often exits in the form of dedicated connections from control system networks into product or services supplier's networks or "cloud monitoring and diagnostics" systems, established to permit routine maintenance of customer equipment and software.

4.4.10 Removable Media

All removable media can contain malware and other attacks, including Digital Video Disks (DVD), Compact Disk Read-Only Memory (CD-ROM) disks, Universal Serial Bus (USB) Thumb Drives, USB hard drives, and even entire laptops and computers re-purposed from IT networks, or computers fresh from a computer vendor. In a sense, removable media attacks and the "bypass the firewall" attacks above are not even attacks on or through a firewall. They are however, attacks through the OT network perimeter that a firewall was deployed to protect, and so must be considered in any discussion of perimeter security.

4.5 Traditional Control-System Security Advice

Traditional control-system security advice, standards, and regulations include measures that try to address these fundamental limitations of firewall technology. This advice assumes firewalls are necessarily porous, and that some attacks will enter control system networks through firewalls. Security advice includes measures to make breaching firewalls more difficult, measures to protect vulnerable control system equipment when the inevitable occurs and some attack breaches the firewall, measures to reduce the risk that people will bypass firewalls either deliberately or accidentally, and measures to detect and respond to attacks when they occur. Each of these classes of measures is described below.

The sum of all these measures is known as a "defense-in-depth" program. Since every protective measure has limitations and sometimes its own vulnerabilities, there is no one thing or combination of things that can be done to prevent all attacks. Instead, the goal of a defense-in-depth program is to make attacks so difficult that would-be attackers either give up, or are slowed down so seriously that targeted organizations have a real chance of discovering attacks and responding to them before any serious damage is done.

4.5.1 Perimeter Hardening

Standard advice for protecting the perimeter of industrial networks includes:

- **Firewalls**: Deploy firewalls between sub-networks at different levels of trust, and within networks at the same level of trust where practical, to separate different kinds of systems and networks, and so make the propagation of attacks and malware within large network more difficult.
- **DMZ**: Create a "demilitarized zone" (DMZ) network between the corporate IT network and the control-system network. Protect the DMZ/IT connection with a firewall, and the DMZ/control-system connection with a firewall. Use different communications protocols to communicate through the DMZ/IT firewall than are used to communicate through the DMZ/control-system firewall. Never forward a message directly from an IT network into the control-system network. When followed strictly, this rule creates a new layer of computers that must be breached "on the way into" the ultimate target, which is sabotage of the industrial control-system network.
- **Different Vendors**: Deploy firewalls from different vendors in layers around a protected network. For example, deploy a firewall from one vendor at the DMZ/IT network interface, and a firewall from a different vendor at the DMZ/control-system network interface. Using multiple vendors reduces the likelihood that a given firewall software defect or vulnerability exists in all the deployed firewalls simultaneously. Using different vendors also reduces the likelihood that any particular error in configuring a vendor's firewalls will be repeated in other vendors' firewall configurations.
- **Deny by default**: Create firewall rules that by default deny all packets, and permit only packets that match specific criteria to enter control system networks or DMZ networks. Put differently, assume, that all packets are attacks, unless the packet matches a rule identifying specific packets that the business needs to flow into protected control-system networks.
- **Deny all connectivity with high-risk destinations**: Do not permit equipment on control system networks and their DMZs to exchange packets with electronic mail servers, any server on the Internet or any other equipment deemed "high risk." When personnel at industrial facilities require access to dangerous destinations, provide that access via dedicated corporate IT computers deployed

physically within the plant boundaries, but connected electrically to the corporate IT network instead of to the control-system network.

- **Outbound controls**: Deny all packets by default, even for packets leaving control-system networks. Modern malware gathers intelligence from compromised equipment and sends that information to attackers, generally via compromised equipment on corporate networks, or via computers across the Internet. If a bit of malware somehow becomes installed on control-system equipment, then controlling the flow of packets leaving control networks makes it more difficult for the malware to report detailed intelligence about the structure and vulnerabilities of the control network.
- **Encryption**: Encrypt communications passing through untrusted networks. Plain-text communications are more easily stolen than are encrypted communications, and more easily tampered with as well.
- **Jump Hosts for Remote Access**: when connecting from a distant laptop or computer into a control system, for emergency remote support for example, terminate all such connections in an intermediate system or "jump host" outside the control-system firewall. The jump host should be thoroughly secured, with measures such as two-factor authentication, the latest security updates, multiple anti-virus vendors and other host-protection measures installed. Permit only required connections from the jump host to the control system through the firewall. Again, the intent is to slow down remote control attacks by making the machine that receives remote control connections as secure as is practical.

4.5.2 Host Hardening

Standard advice for protecting the network of hosts and devices inside an industrial network perimeter includes:

- **Anti-malware**: Anti-virus systems identify high-volume malware by searching executable files and libraries for matches on libraries of "signature" rules. Anti-virus systems cannot be deployed universally on control systems, though. Anti-virus vendors generally do not support all of the different kinds of computer and operating systems on control networks, and the constantly-updated anti-virus signatures introduce a risk of "false positive" matches that falsely identify essential control system software as viruses. A false positive match on an essential control-system software component quarantines or otherwise impairs the operation of that essential component. Anti-virus systems can also consume CPU, memory and disk access resources essential to safe or reliable operation of the control system and the physical process. Application control/whitelisting is an anti-malware alternative that seeks to identify malware by comparing executable files to lists of "allowed" executables.
- **Security updates**: Software updates or "patches" are changes or updates to programs and applications issued by operating system, application or control

system vendors that close known security holes. Security updates generally cannot be deployed promptly on safety-critical or reliability-critical networks, because the new, untested code in those updates represents potential safety and reliability risks. For example, in some industries, any change to the code in critical components necessitates a re-certification of those components through certification authorities before it is legal to run the changed code.

- **Host hardening**: Host hardening consists of un-installing unnecessary components and code, disabling unnecessary operating system services, physically disabling unnecessary USB, network and other ports, applying host firewalls to drop packets to unauthorized TCP and UDP ports and many other measures. These measures serve to reduce the "attack surface" on control system hosts by reducing the amount of code that is installed, running or otherwise exposed to attack on the host. Determining what is "unnecessary" though, can be very difficult. Control system vendors generally do not publish a description of the operating system components and services that are essential to the correct operation and emergency operation of their control system products.
- **Password and account management**: These measures provide each control system user with their own accounts and passwords, require that these passwords be changed regularly, and minimize permissions for each user or role to limit authorized users to those actions the user is permitted to carry out. Password and account management on control systems can be very difficult though. Many control-system measurement and other devices do not support multiple users. More importantly, passwords cannot be permitted to interfere with emergency operations, and passwords can be very difficult to remember when panic sets in during a life-safety emergency.
- **Encryption**: Encryption and authentication of communications between hosts in control system networks can make these networks more resistant to certain kinds of attacks, but can also serve to make those networks more difficult to configure correctly, to manage, and can serve to impair certain kinds of emergency response.

In short, network perimeter protections are generally perceived as safer to apply to control system networks than host protections. Control systems are generally designed to run safely, indefinitely, even if connections through a network perimeter fail due to mis-configuration of perimeter defences. Host hardening provisions though, all have the potential to interfere with both normal and emergency operations of control system hosts.

4.5.3 Personnel

Standard advice for protecting control system networks from attacks in the form of people walking up to control system equipment and mis-operating that equipment include:

- **Physical perimeter**: All safety-critical and reliability-critical components of both the physical process and the control system generally reside within a physical security perimeter protected by "guards, gates and guns." The entire cyber-perimeter resides within this physical perimeter as well.
- **Background checks**: Permit past the physical perimeter only those individuals who have passed a criminal and/or terrorist background check.
- **Detailed forensic auditing**: Provide each user with their own account and password, and log all activities both locally and to a physically secure remote location. Compare local and remote logs periodically to detect tampering. This logging serves to deter insider attacks, by increasing the likelihood that any deliberate mis-operation of the physical process can be traced to a guilty party for prosecution after the event.
- **Video monitoring**: Video cameras throughout an industrial site serve not only to provide physical security responders with real-time monitoring of their physical perimeter protections, but recordings of those cameras provide additional deterrence to deliberate mis-operation. Even if an insider steals another user's password, comparing online audit records with video records can reveal which person carried out mis-operation of the control system.

4.5.4 Intrusion Detection

Intrusion detection is seen as the pinnacle of every IT-centric defense-in-depth program:

- **Signature-based network intrusion detection (NIDS)**: examines packets on a network for matches against a database of known attack "signatures."
- **Network intrusion prevention**: intrusion prevention systems are generally signature-based NIDS with the ability to drop attack messages or close connections in which attack messages are detected.
- **Anomaly-based NIDS**: "learns" what normal traffic is over a period of time, and raises alerts when "significant" anomalies are detected. Anomalies may include new kinds of communications between hosts, unusual volumes or frequency of known communications, and unusual content packets whose protocols the NIDS may have some understanding of.
- **Host intrusion detection**: "learns" what normal behavior looks like on different control system hosts over a period of time, and raises alerts when "significant" anomalies are detected. Anomalies may include the creation of new files with unusual names, or in unusual locations, and the creation of new processes with unusual characteristics.

Fundamentally, all IT perimeters are assumed porous; after all millions of pieces of electronic mail, web pages and other messages are permitted into large IT

networks every day, and in spite of the best efforts of firewall and other filters, some of these permitted messages contain attacks. Fundamentally, all IT interiors are software. All software has vulnerabilities and in practice, all software can be hacked, even security software. Together, this means all IT networks are expected to be compromised, regularly. Intrusion detection is seen as the answer to this unacceptable condition. Intrusion detection "pits our experts against theirs." "Our" experts constantly monitor intrusion detection systems and alerts, investigate those alerts, determine which are real and which are false alarms, identify compromised equipment, and activate intrusion response plans and teams to isolate the affected equipment, erase that equipment and restore it from backup. Intrusion detection and incident response are seen as absolutely essential to the integrity of fundamentally porous, soft IT networks.

Control-system networks are different though.

4.5.5 Limitations of Traditional Advice

For the first decade of the modern control-system-security initiative, starting in roughly 2002, security advice for industrial control systems encouraged security practitioners to apply standard, IT-centric security systems to control networks, as much and as thoroughly as was possible. This advice recognized limitations of the IT-centric approach, especially the impact of such security measures on safety-critical and reliability-critical systems. Physical security, personnel security, firewalls and NIDS were seen as the easiest protections to apply "after the fact" to existing control systems, because none of these measures affect the flow of network messages or the execution of applications on hosts within sensitive control system networks. All host-based systems as well as network intrusion-prevention systems were seen as intrusive: potentially altering the correct flow of messages and execution within critical control system components.

All that said, the advice to practitioners was still to, as much as possible and as thoroughly as possible, apply IT-centric security advice to control system networks. Control system vendors were encouraged to design new versions of their products to work with and tolerate the operation of "intrusive" host-based IT-centric protections, such as anti-virus systems and security update programs. Intrusion detection vendors were encouraged to design a knowledge of control system hardware, software and communications protocols into their products. This generation of advice essentially said that if we could only *invent* some way of applying IT-centric security mechanisms to control system networks and components, then all would be well.

More recently, expert advice is moving away from this position. Even if we apply IT-centric cyber-security measures to control system networks, we see unacceptable risks. Since control-system firewalls are inherently porous, since the interior of all control-system networks contains many computers and software, and since all software can be hacked, the compromise of control-system networks, like

IT networks, is inevitable. The classic IT response to this unacceptable situation is intrusion detection. Intrusion detection though, takes time. A Ponemon Institute study in 2013 (Ponemon 2013) is typical of many such studies; it found that malicious cyber breaches took an average of 80 days to detect, and 123 days to resolve. In the world of industrial control systems, this means that, for at least all of the time taken to detect the breach, a malicious attacker has control of equipment on critical control-system networks.

This is considered an unacceptable risk by almost all owners and operators of industrial control systems. Expert opinion in the last several years has evolved to recommend that industrial control-system security programs be based on a much stronger foundation of protection from intrusion than is accepted practice for IT networks, or is even possible for IT networks.

4.6 Modern Alternatives to Firewalls

Since about 2010, new industrial cyber security standards and guidance, as well as older guidance that has been updated, document unidirectional gateways (Waterfall 2011) as the modern alternative to firewall perimeter protections for industrial control systems.

4.6.1 Unidirectional Gateways

An example unidirectional gateway deployment is illustrated in Fig. 4.2.

The unidirectional gateway in the example replaces the IT/OT firewall and DMZ network connecting an industrial network to a corporate network, and makes data from an industrial process historian[2] database available to corporate users and applications.

All unidirectional gateways are combinations of hardware and software. A transmit (TX) hardware module contains a fiber-optic[3] transmitter, but physically contains no receiver. A receive (RX) module contains a fiber-optic receiver, but physically contains no transmitter. A short fiber-optic cable connects the two modules. The result is a system able to transmit information out of a protected industrial network, but physically unable to transmit any information at all back into

[2]A process historian is a database designed and optimized to store large volumes of time-stamped data. For readers more familiar with relational databases, the truism is that "a relational database can be configured to do everything a historian database does, but the relational database would need thirty times as many servers."

[3]A minority of unidirectional hardware uses electrical signalling, but optical signalling is widely preferred. All electrical circuits are circular after all, and risk encoding information in the reverse electrical flow.

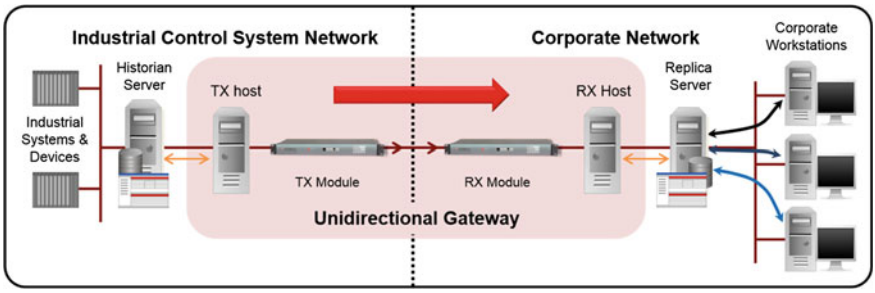


Fig. 4.2 Unidirectional historian replication

that network. The TX module has no way to determine if the RX module is activated or is listening at all. The TX module always transmits "blind."

The software portion of a unidirectional gateway is called an "agent" or a "connector" and makes copies of industrial servers, or emulates industrial devices. In Fig. 4.2, the software illustrated makes a copy of the industrial historian database. The TX agent software in the industrial network connects to the industrial database over a conventional two-way connection, with a user name and password, and asks the industrial database for time-stamped, historical data. The software transmits that data to the external, corporate network through the one-way hardware. On the corporate network, the RX agent software connects to another historian database, and asks that database to store the time-stamped data received from the one-way hardware. In effect, the unidirectional gateway software produces a corporate replica of the industrial historian, with the most recent data in the corporate replica historian generally less than one second older than the most recent data in the industrial historian. Corporate users and applications that need access to the latest industrial data can query the replica historian for the data, and be confident of receiving the same answer as would have been provided by querying the industrial historian.

4.6.2 Unidirectional Gateway Security

Standards are evolving to recommend unidirectional gateways, because the gateways offer far greater protections for the safety and reliability of industrial networks than firewalls are able to provide. If a firewall were used to mediate access to an industrial historian from a corporate network, corporate users would need to send query messages into the industrial historian, on the industrial network or a DMZ network, in order to retrieve data. Firewalls are routers—if the query message passes the firewall's filter criteria, the firewall would forward the query to the historian. If the query is legitimate, the historian replies with the requested data. If the query is an attack message that manages to deceive the firewall's filter, the historian is under attack, right through the firewall.

A historian on a unidirectionally-protected network is physically unable to receive any message at all from the less-trustworthy corporate network. No cyber-attack, however sophisticated, can physically turn a photocell into a laser, or vice-versa. Corporate users and applications send their queries to the replica server. Any successful attack on the replica server is cause for alarm in the IT security domain, but is physically unable to affect the control-system historian or via the historian, the control system network in any way.

In addition, firewalls forward messages, but, depending on the vendor, unidirectional gateways generally do not. If some remote-control malware gets a foothold on an industrial network, for example by propagating via removable media, that malware generally tries to establish a connection with a command and control center on the Internet in order to forward illicit packets through firewalls to the Internet. Any firewall that permits such packets permits malware to exfiltrate data to the Internet, and generally permits that malware to receive remote-control commands from the Internet over that same communications channel.

But consider the case when malware somehow infects the control-system network in Fig. 4.2. The unidirectional gateway software inside the industrial network is a client of the historian database, similar to how a spreadsheet is a client of a relational database. The client requests specific data from the database and discards all of the messages used to acquire that data, similar to how a spreadsheet acquires data from a relational database. The gateway software/client then transmits a serialized version of the historical data to the external, corporate network, similar to sending the spreadsheet full of data out to the corporate network.

If the gateway's TX agent software receives a rogue Domain Name Server (DNS) request, or web page request, what will the software do with that message? Well—what would a spreadsheet do with such a message? The software is a client, is not a router, nor a DNS server, nor a web server. The software has no choice but to discard the message, not because there is a rule to discard the message, but because the software genuinely has no idea what to do with such a message/request.

In short, firewalls forward messages, and unidirectional gateways generally do not. This means that not only do the gateways physically prevent any message from a less-trusted network from reaching an industrial network to put that network at risk, the gateways also pose much greater barriers than do firewalls, to any communication at all from malware in an industrial network seeking to exfiltrate data to a command and control center on an external network.

4.6.3 Emulating Devices

Not all industrial networks host historian databases or relational databases. Many businesses with industrial operations host only one enterprise-wide historian in a central location on the corporate network, and that historian pulls data directly or indirectly from industrial devices in one or more industrial networks. In this case,

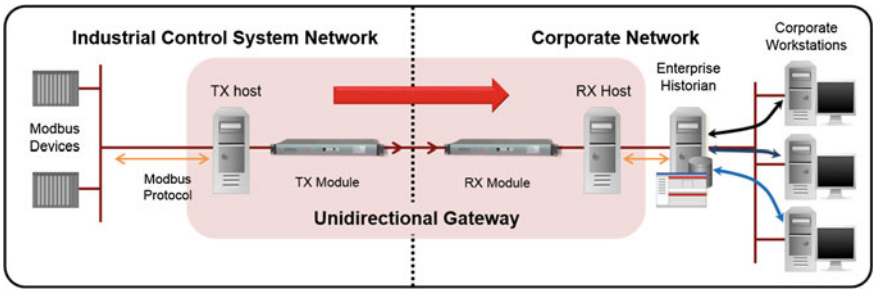


Fig. 4.3 Modbus device emulation

unidirectional gateways are generally configured to emulate industrial devices so that the corporate historian can poll the emulated replicas.

For example, Modbus is a protocol commonly used to communicate between historian databases and industrial devices. Figure 4.3 illustrates unidirectional Modbus/TCP device emulation.

In the figure, the gateway software on the TX host polls Modbus devices on the industrial network using the bi-directional Modbus/TCP protocol, requesting current measurements and device information. Measurement and state information is extracted from the Modbus responses, and all of the Modbus response messages are discarded. A serialized version of the extracted data is transmitted to the gateway software on the RX host. The RX host keeps this information in memory, and emulates the Modbus devices on the industrial network. The enterprise historian uses the native, bi-directional Modbus/TCP protocol to poll the emulated devices. When Modbus poll requests are received by the gateway software, the software responds to those requests in the same way as the original industrial devices would have.

4.6.4 The FLIP

Many unidirectionally-protected networks though, still require that data of some sort enter the network through the control-system perimeter routinely. Consider, for example, anti-virus signature updates. Even if anti-virus signature updates cannot be applied to all control-system equipment without first testing the signatures for false positives or other problems, anti-virus signatures can and should be applied routinely to non-critical equipment on control system networks, and many control-system owners and operators require automatic updates of such signatures at least several times per week.

Unidirectionally-protected sites generally meet this need either with a program of manual updates, where anti-virus signatures are burned to write-once compact disks and manually loaded on to a test-bed, or with a unidirectional FLIP product.[4]

[4]At present, FLIP technology is available only from one vendor, Waterfall Security Solutions.

FLIP technology is a kind of unidirectional gateway; a FLIP is able to transmit information only unidirectionally. A FLIP, though, has the ability to reverse the orientation of the unidirectional medium. A FLIP can transmit unidirectionally out of a protected network, or into that network, on a schedule.

A common schedule for anti-virus updates is to reverse orientation briefly, say for 10 min at a time, several times per day. The scheduler for the FLIP is not accessible via either the control-system network or the corporate network, and so cannot be controlled or compromised from either network. Unidirectional software on each network though, is able to detect the orientation of the FLIP and can take appropriate actions when the orientation reverses. For example, a unidirectional anti-virus connector can detect when the FLIP is oriented into the control system network, and can use that reversal of direction as a trigger to check if updated anti-virus signatures are available, and if such updates are available, download, verify and transmit them into the protected control-system network for re-verification and deployment.

FLIP technology is also used routinely to transmit production orders into batch-oriented control systems, security updates into control-system test-beds, and signed, control system configuration updates into live control systems, such as might be produced from time to time by control system or equipment vendors providing remote monitoring and diagnostics services to an industrial site.

Even though the FLIP can reverse periodically, FLIP technology is still far more secure than a firewall. Every FLIP is a unidirectional gateway, and unlike firewalls, gateways do not forward IP messages or other kinds of messages from one network to another. To attack a server through a firewall, an attacker needs only to find an attack packet that the firewall is willing to forward into the server. To attack a server on a FLIP-protected network is a multi-stage process. An attacker must:

1. Find a way to compromise the server running the unidirectional gateway agent software on the corporate network,
2. Find a way to propagate that attack through the unidirectional hardware, while that hardware is oriented into the control system network, to compromise the server running the unidirectional gateway agent software on the control system network, and
3. Find a way to reach into the control system network from the compromised gateway server and attack the control network.

This is a three-stage attack, rather than the single stage needed to reach through a firewall. In addition, the second and third stages of the FLIP attack are singularly difficult, because while the FLIP is oriented into the control-system network, no feedback from the attack can return to the attacking network. When the FLIP reverses orientation, feedback is possible, but no new commands or attacks are possible. In addition, FLIP technology is routinely installed as illustrated in Fig 4.4, such that the unidirectional software components are installed on different servers on the corporate and industrial networks. As a result, it is not possible for an attacker to see any feedback from steps (2) of the attack or gather any intelligence about how to carry out step (3) until step (3) is successful. This is a “flying blind”

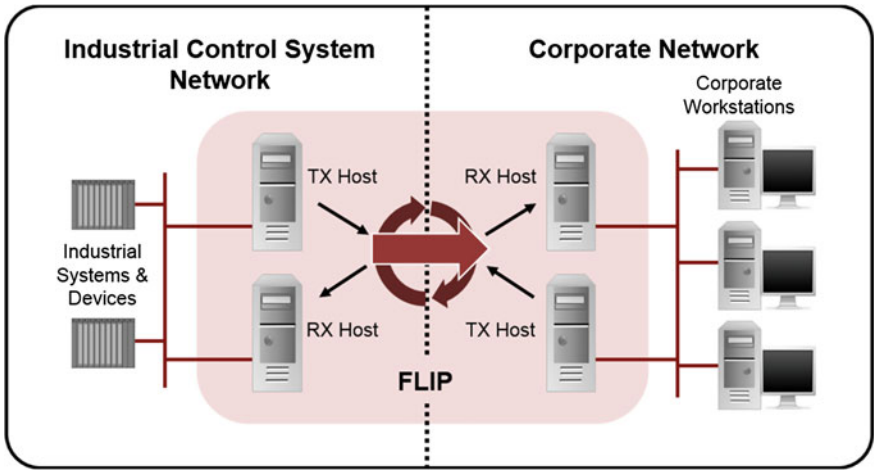


Fig. 4.4 Reversible "FLIP" gateway

problem—the attacker is not able to gather intelligence about how best to carry out step (3) until step (3) is complete.

In short, it is possible to attack control system through the FLIP, but such attacks are very difficult. The most credible such attack relies on a compromised insider on the control system network, deliberately feeding information to the attacker about the design of the industrial network and the progress of the attack, or actively assisting the attacker by planting malware on the industrial network to overcome the "flying blind" problem. In addition, conventional remote-control attacks, such as are launched by common viruses and botnets, are ineffective through a FLIP. The FLIP prevents any interactive bi-directional session that might permit a remote attacker to operate malware planted on the control system network.

4.6.5 Inbound and Outbound Gateways

In certain circumstances, it is imperative that control system components receive communications continuously from components outside of a control-system cyber perimeter. For example, in an electric grid, a grid control center, usually called a "balancing authority" or "transmission system operator" must pull information every second or two from all electric utilities in a specified geography, and must issue new generating set points just as frequently to generating utilities in that same geography. Because electric power cannot be stored for significant lengths of time at grid scales, the authority must balance generating capacity against electric loads continuously. Other examples of continuous remote control requirements include remote water and petrochemical pumping stations as well as electric substations,

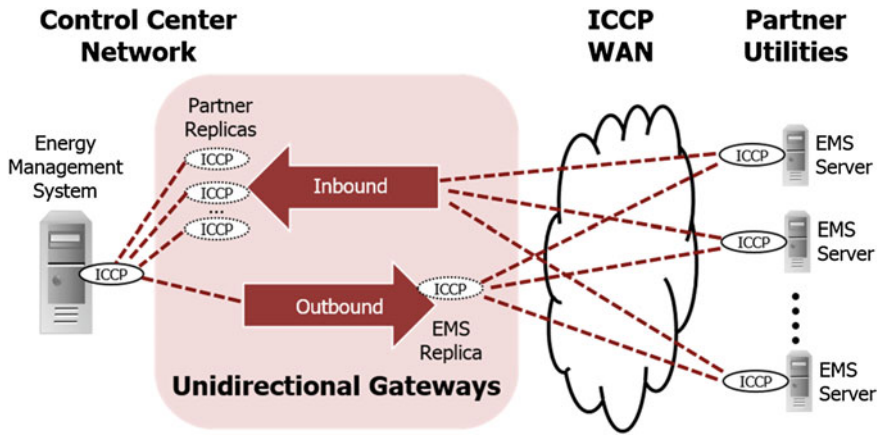


Fig. 4.5 Inbound/outbound unidirectional gateways

which are generally distant, unstaffed sites that must be continuously and remotely monitored and controlled.

In these applications, inbound/outbound unidirectional gateway combinations are deployed. These deployments consist of a pair of unidirectional gateways, one oriented to replicate servers into the protected site, and one oriented to replicate servers out of the site. An example of such a deployment at an electric grid control center is illustrated in Fig. 4.5.

To simplify Fig. 4.5, the hardware and software components of each unidirectional gateway have been collapsed into a single "arrow" icon. Each of the inbound and outbound gateway icons must be understood to contain all of TX and RX hardware modules, and TX and RX hosts running gateway software on either side of the modules, as was illustrated earlier in Fig. 4.2.

In this example, the control-center network of the balancing authority or transmission system operator runs an energy management system (EMS), as does each of the utility partners. The control-center EMS software gathers information from all of the partner utilities, generally over a dedicated Wide-Area Network (WAN), using the Inter Control Center Protocol (ICCP). The control-center EMS decides whether, by how much, and in which geography to adjust the amount of generated power, and creates new setpoint values for each of the generators in each of the partner utilities.

Neither of the unidirectional gateways in Fig. 4.5 forwards ICCP messages; instead, each replicates one or more of the ICCP servers associated with an EMS. The outbound gateway replicates the control center's ICCP server to the ICCP WAN at the bottom of the diagram, so that partner utilities can poll the replica to gather new generation set points. The inbound gateway at the top of the diagram, replicates all of the partner utilities' ICCP servers, so that the control-center EMS can poll those replicas to understand how much power is being produced and consumed by each utility, in each part of the geography.

Inbound/outbound gateways are deployed when the only alternative cyber perimeter protection is a firewall. Like the FLIP, inbound/outbound gateways can be breached from an outside network in theory, but the attack involves a three-step process. Like the FLIP, for the last two of the steps, the attacker is blind to whether an attack stage has succeeded, and is unable to recover intelligence from the targeted control-center network to assist in the attack, until the attack has already succeeded in compromising the EMS or its ICCP server. In practice then, this class of attack is only practical when there is an insider assisting the attacker.

4.6.6 Unidirectional Gateway Security

No defense is perfect, and unidirectional security gateways and their related technologies are no different. For example, when penetration testers come up against a unidirectional gateway in a network architecture, their first reaction is to try to find a way around the gateway, because there generally is no way through it. Rogue wireless routers, alternate connections between networks, and even old-style dial-up telephone lines to enable access for vendors to their specialized equipment are all connectivity paths around unidirectional gateways, or firewalls for that matter. Physical attacks are also a path around gateways—every person permitted to carry USB sticks, laptops or even brand new computers into a facility is a potent attack path.

In a sense, this is not surprising. The purpose of a unidirectional gateway deployment is almost always to "raise the bar" for attackers. With a gateway deployed, an attacker can no longer sit in their basement on the other side of the planet, working their way deeper and deeper into an industrial network by interactive remote control. With a unidirectional gateway deployed as the only connection between an industrial network and less trusted networks, the only classes of attack effective against the protected site are physical attacks. To attack a unidirectionally-protected site, an attacker must either put themselves in physical danger, by attempting to physically break through the industrial site's physical perimeter, or they must deceive or coerce another person into physically carrying an attack into the site for the attacker.

4.7 Remote Access

Remote access is a controversial aspect of industrial perimeter security. Proponents of remote access point to productivity gains from access to control system experts "anytime, anywhere," and access to control-system vendor expertise via the vendors' central monitoring and diagnostic centers. Opponents point out that every interactive remote control setup can be breached, and that the consequences of such compromise are far greater for control system remote access than from remote access to IT networks.

4.7.1 Compromising Remote Access

Consider a modern, remote-access system protected according to IT security best practices:

- Remote laptops connect to a jump host using a VPN with a strong encryption algorithm and a long key.
- Before connecting, the VPN software reports the laptop's anti-virus and security update posture to the control system's VPN server, and the server permits the connection only if the very latest signatures and security updates have been installed on the laptop.
- The VPN is configured to prohibit "split tunneling," meaning that while the VPN is active, the laptop is permitted to communicate only with the control system's VPN server, and not with any other network, especially not the Internet.
- Network intrusion detection software is deployed on control system and the corporate IT network.
- All login sessions on the jump host must be via two-factor authentication.
- Detailed logging is configured for all actions on the jump host.
- The jump host is kept completely and automatically up to date with the latest anti-virus signatures and security updates.

Such a configuration is compliant with best practices as described in a variety of IT and ICS security standards, and in spite of such compliance, is easily breached. The simplest attacks target the remote laptop that is the endpoint of the VPN connection, rather than the encryption algorithm, keys, software, or protocols.

An example of such a simple attack on an IT-protected remote access station looks like this:

The attacker writes a small amount of code, in the form of malware that reaches out to the Internet to download additional attack tools.

- The attacker does some homework on her target's remote workforce using social networking sites, and crafts an electronic mail message with the new malware attached, a message that is very likely to deceive one of the remote workers into activating the attachment.
- The attachment installs itself on the laptop, and downloads additional attack tools.
- None of this activity triggers an anti-virus alert. This is the first time this new malware has been used, so there is no anti-virus signature for it.
- The malware waits until the remote user establishes a VPN connection, opens a remote desktop session and logs in using the two-factor authentication mechanism.
- The malware then creates an invisible virtual screen, moves the remote desktop window to the invisible screen, and shows the user a message saying "Remote Desktop has become unresponsive. Checking for a solution."

- The malware then sends images of the invisible remote desktop window to the remote attacker across the Internet and permits that attacker to send mouse movements and key strokes to the invisible window.
- The malware defeats the split-tunneling protections of the VPN by accessing the network hardware directly, or by routing the connection to the command and control center through the VPN and out to the Internet from the network that is the destination of the VPN.

Producing this kind of malware is requires a modest investment in writing code. None of the code in this malware is particularly difficult to produce. This class of attack provides the attacker with remote control of the laptop's remote desktop session after that session has successfully connected into the control-system jump host. No classic IT-security protections prevent this attack:

- Anti-virus systems do not activate, because the anti-virus vendor's Internet honeypots have not seen this attack code before, and so no signature exists for the attack. Anti-virus systems are reasonably good at detecting high-volume attacks, but are not effective at detecting targeted attacks.
- Security updates did not help, because the attack did not take advantage of any software vulnerability. The attack was installed and given administrative privileges through social engineering, not by attacking known or zero-day vulnerabilities.
- The encrypted VPN did not help, because the endpoint of the encrypted VPN tunnel was compromised. Encryption cannot protect against the compromise of an encrypted endpoint.
- Two factor authentication did not help, because the remote desktop session was taken over only after the authentication credentials were used.
- The control-system site's intrusion detection facilities did not detect the attack because there was nothing suspicious about the attack. This remote user logs in routinely from this laptop, via a VPN, and reconfigures the control system. That the apparently-legitimate user is mis-configuring the control system rather than configuring it correctly is a subtlety the intrusion detection system is unable to identify.

Corporate IT security teams are well aware of the possibility of this class of attack, but those teams tend to focus on attacks where stealing data is the objective, not sabotage. To steal data, an attacker must search for, find, and extract valuable data from the enterprise, and this searching and extraction activity does have clear patterns of activity that can be recognized by intrusion-detection systems. Sabotage of control system assets is subtler. Often, such sabotage can be carried out without an attacker accessing anything other than the computers and applications that are accessed routinely via the compromised remote laptop.

4.7.2 Remote Screen View

Unidirectionally-protected sites generally forbid interactive remote access as an unacceptable risk. To support remote vendors and their monitoring and diagnostic services, the sites may deploy unidirectional remote monitoring and remote screen view (RSV). Remote monitoring for vendors is a straightforward application of unidirectional gateways, replicating whatever industrial servers the vendors may need to monitor.

For example, such vendor monitoring is configured routinely for steam and gas turbines. Turbine vendors generally provide warranties and support contracts for their rotating equipment only if the vendors can monitor the equipment continuously, and adjust the equipment occasionally, when significant vibration or heat distribution anomalies are detected. Without monitoring and adjustment, such anomalies risk growing over the course of weeks and months into catastrophic failures of the rotating equipment.

When a vendor detects a problem in a control system component via the replica servers, that vendor contacts the site and schedules a remote screen view appointment. At the appointed time, the site calls the vendor back, and activates remote screen view.

Remote screen view is a technology that, like remote desktop, takes pictures of the screens of one or more control system workstations and transmits those images out of the control system network via unidirectional gateway hardware. On the external network, the vendor is able to see the screen of the internal workstations, but cannot influence those workstations in any way. An engineer at the control system site on the phone with the remote expert cooperates with that expert in the process of adjusting control system parameters. The vendor sees the process as supervising the site, to ensure that a complex problem is corrected to the vendor's satisfaction. Personnel at the site see the process as supervising the vendor, to understand what problem the vendor corrected and how. In short, remote screen view is used routinely for supervised, intermittent remote access by vendors and other third parties.

4.7.3 Central Engineering Sites

Some enterprises with multiple industrial sites have centralized their control-system engineering teams. These engineers at a central site require continuous remote access into whatever industrial sites are the foci of current engineering projects, and are trusted to work on control system assets unsupervised. Remote screen view is seen as impractical for this kind of continuous remote access by trusted insiders. Instead, many enterprises use unidirectional gateways to mediate the majority of IT/OT data movement, and extend their plant networks to central engineering sites via VPNs deployed over dedicated WAN connections.

While every extension of a reliability-critical or safety-critical network to another site impairs the security of the critical network, enterprises deploying such extensions take a number of measures to minimize security risks:

- Connections to central sites are via dedicated WAN infrastructure, not via corporate networks or the Internet.
- Connections between sites are encrypted.
- The central site is protected with the same class of physical and personnel security measures as are used to protect the industrial site.
- Equipment on the central extension of the industrial network is managed the same way as equipment on the industrial network. In particular, no such equipment is permitted to read electronic mail, browse the Internet, or carry out other dangerous activities, and the only connection between a less-trusted network and any industrial network or the central engineering network extension, is via unidirectional gateways.

In practice then, every engineer at the central site requires routine access to at least two computers: one computer is part of the industrial network extension and is used to access industrial control system components, and the other is part of the corporate IT network and is used to carry out dangerous activities such as reading electronic mail. Delegating dangerous activity to a corporate IT asset minimizes the possibility of an Internet-based compromise of the remote engineering endpoints on the central extension of the industrial network.

4.8 Evolving Standards and Best-Practice Advice

Cyber attacks and cyber attack tools only become more sophisticated over time; what was yesterday's "advanced" attack is today's "script-kiddie" attack tool. As a result, control-system security advice must continue to evolve, to address threats of steadily increasing sophistication and effectiveness.

The first generation of industrial control-system cyber security standards and guidelines focused on insider attacks and common malware. Insider security controls recommended in this generation of advice focused on password management, account management and role-based access, as well as the usual personnel background checks and physical security measures. Malware prevention focused on anti-virus systems and security updates, which were controversial "constant change" measures in the control-system world of engineering change control for critical industrial networks.

Late in the first decade of the twenty-first century, targeted attacks began to be recognized as the most serious threat to IT networks and to control system networks. The IT approach to defending against such attacks was defense-in-depth and especially intrusion detection, while the control-system approach focused on improving protective measures for control system networks, including unidirectional gateways at network perimeters.

4.8.1 NERC

CIP

Starting with version 5, approved in 2013, the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) standards[5] require significantly different protection profiles for unidirectionally-protected networks vs. firewall-protected networks. The standards define "External Routable Connectivity" (ERC) as:

> **External Routable Connectivity**: *The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter* via *a bi-directional routable protocol connection.*

The word "bi-directional" in this definition excludes all control system sites whose only interaction with external networks is either via unidirectional gateways, or via more-primitive "non-routable" connections, such as leased or dial-up serial connections. NERC CIP V5 sites with ERC are required to conform to some 127 requirements, while sites without ERC have only 89 requirements. In effect, the use of firewalls at a NERC CIP site increases the number of security requirements at the site by 38: all of the requirements that take effect only if the site has ERC.

Thus, while the NERC CIP V5 and later standards do not require the use of unidirectional gateways at any NERC CIP site, the standards do encourage the use of unidirectional protections by reducing the compliance burden for unidirectionally-protected sites.

In addition, while NERC CIP V5 and V6 standards allow remote access to the most critical classes of control-system networks, provided that IT-style security best practices are followed, these rules are being re-examined. At this writing, the Federal Energy Regulatory Commission (FERC), from which NERC draws its regulatory authority, has issued a request for comments as to whether existing NERC CIP provisions for remote access provide acceptable levels of security.

4.8.2 ANSSI Standards

The French Agence nationale de la sécurité des systèmes d'information (ANSSI) cybersecurity standards are advice for existing control-system networks, and have the force of law for newly-deployed networks. The standards define three classes of industrial control-system networks:

- Class 1 networks are in a sense expendable: French society does not depend on such networks for critical functions. For example, a washing-machine

[5]While NERC calls the CIP publications "standards," these documents in fact have the force of law for most North American utilities that are part of the NERC-defined Bulk Electric System.

manufacturer's control network may be critical to the manufacturer, but French society is largely unaffected if the network is sabotaged.
- Class 2 networks are important to French society: there are significant consequences for citizens if networks such as those at a medium-sized water treatment plant, or at a large chemical plant, are breached.
- Class 3 networks are critical to French society: there are generally life-threatening consequences for compromised networks, for example, railway switching networks, or the safety-instrumented networks at a large chemical plant.

The ANSSI standards state that for class 2 networks, communications connections to any less-critical network "should be unidirectional" towards the less-critical network. For class 3 networks, connections to any less-secure network "shall be unidirectional" and that unidirectionality "shall be guaranteed physically."

In addition, the ANSSI standards "strongly discourage" remote access for class 2 networks, and forbid such access for class 3 networks, excepting only "devices that physically guarantee the impossibility of interacting with the class 3 network," devices such as remote screen view via unidirectional gateways.

4.8.3 Other Standards

A variety of other recent standards and advice either document, encourage or require unidirectional gateways. For example:

- The International Society of Automation (ISA) SP-99/International Electrotechnical Commission (IEC) 62,443 family of standards documents unidirectional gateways as part of a defense-in-depth program.
- The American Nuclear Regulatory Commission (NRC) 5.71 and the Nuclear Energy Institute (NEI) 08-09 standards effectively require unidirectional gateways. The standards permit firewalls, but require such a large set of compensating measures to be deployed for firewall-protected nuclear generators, that in practice, all American nuclear generators have deployed unidirectional protections.
- The American National Institute of Standards and Technology (NIST) 800-82r2 standard discusses unidirectional gateways and positions them within a control-system defense-in-depth program.
- The Qatari control system regulations for the electric sector recommend unidirectional gateways.
- The European Union Agency for Network and Information Security (ENISA) positions unidirectional communications as providing "an even higher level of protection" than firewalls coupled with intrusion detection systems.

The clear trend is that modern standards and regulations generally document, encourage or require unidirectional gateways, and the more sensitive is the protected network, the stronger the rule for gateways is likely to be.

4.9 Analysis: Why Are the Lights Still On?

While unidirectional gateways are deployed at an increasing number of critical infrastructure control-network perimeters, deployment of such gateways is far from universal. Given the vulnerability of traditional corporate networks, firewalls and industrial networks to remote-control, cyber sabotage attacks, why have there not been more high-profile, targeted attacks on industrial networks? In short: why are the lights still on?

Exert opinion holds no consensus in this arena. The majority of publicly-disclosed cyber-security incidents for industrial processes are common malware that has somehow infected equipment on a control system network. Such malware is generally designed to steal credit card information, or use compromised equipment for distributed denial of service (DDOS) attacks, or to send out spam. In some such infections, the only consequence for the industrial system is the cost of identifying compromised equipment and restoring it from backup. In other situations, side effects of the malware are such that control system components become confused or impaired, and the site must shut down the physical process while the infection is removed on an emergency basis. Such shut-downs are generally costly. Lost production is always costly; it may take days or more to clean out compromised computers, and it make take additional days to carry out a site start-up again and bring the site back to full production.

Targeted attacks, where perpetrators deliberately try to shut down industrial processes or damage equipment, are less common, and all cyber security incidents on control system networks are less common than are such incidents on Internet-exposed corporate networks. Some experts maintain that the comparatively small number of reported attacks with significant physical consequences demonstrates that existing IT-style defenses deployed at industrial sites are by and large adequate to the needs of protecting those sites.

Other experts disagree. Many industrial sites are protected very poorly; some sites have even connected their control systems directly to the Internet, and are therefore searchable via tools such as Google and Shodan. Password guessing on such sites has yielded remote control of those sites to security researchers, and the use of weak or default passwords for the control system components was thus exposed. It seems illogical that these primitive levels of security are responsible for the small number of reported industrial incidents.

Some experts maintain that the low number of reported incidents is because there are no mandatory, public reporting requirements for industrial incidents in most jurisdictions, while many jurisdictions have requirements for public reporting of all privacy breaches. These experts argue that there are large numbers of unreported

industrial incidents. Other experts point out that, given what limited data is available, it seems unlikely that there are anywhere near as many serious, targeted industrial cyber security incidents as there are serious, targeted corporate, and government cyber espionage incidents.

Yet other experts maintain that the comparatively small number of industrial cyber security incidents with serious consequences is due to a lack of motive for such attacks. State-sponsored and state-sanctioned actors are responsible for the most sophisticated cyber attacks, but many nations have made it clear that any significant sabotage of societally or militarily critical infrastructure will be seen as an act of war. This acts as a deterrent for the state-sponsored cyber sabotage attackers. Terrorist groups are motivated by publicity; their objective is, after all, to terrorize a population. Sabotage of critical infrastructures may not be seen by such groups as terror-inspiring as bombing a church.

Hacktivists and organized crime are a concern though. Hacktivists have not yet carried out public attacks on control systems operating unpopular industrial sites, but the capability to breach control system defences are widely available. Organized crime is generally motivated by profit, and there does not yet seem to have emerged a reliable profit motive for sabotaging infrastructure. This may be changing. Ransomware encrypts and disables computers until a ransom is paid, which could start to target critical infrastructures. Infected sites could be given a choice between multi-day outages while infected equipment is erased and restored from backup, or multi-million dollar ransoms. Criminal groups could also target industrial sites to realize gains on commodity futures. For example, if a large refinery was targeted and shut down during a period of peak demand for gasoline, the value of gasoline futures would increase dramatically. A criminal organization able to cause such outages for reasons that appear to be normal failures to the refinery operator might profit significantly and repeatedly from such outages. For that matter, there is no way to verify that such attacks are not already occurring.

Targeted attack tools and capabilities have proven very effective at breaching both IT and control-system networks. These targeted attacks now constitute part of the pervasive threat background that every IT and control-system owner and operator must anticipate. Motivations can change in a heartbeat, literally. Attack capabilities evolve much more slowly. Prudent owners and operators of critical industrial control-system networks are deploying protections against pervasive attack capabilities, not motives-of-the-moment.

4.10 Summary

Traditional control-system security advice was focused on insiders and common malware. In large part, such advice was focused on firewalls, encryption, anti-virus systems, security updates, host hardening and password management. This advice is being updated, addressing the risk posed by widely-understood and widely-available targeted attack techniques and tools. Modern advice positions unidirectional

gateways as strong cyber perimeter protections against remote-control, targeted attacks. At least one layer of unidirectional protections between the Internet and the most sensitive control system networks breaks the chain of network and system connections that permit remote control attacks.

4.10.1 Emerging Issues

At this writing, a number of issues are being considered by forward-looking sites and regulatory authorities:

- FERC is looking at whether existing IT-style remote access protections in NERC CIP V5 are adequate protection for the North American Bulk Electric System (BES), given that these protections are easily breached by anyone able to write a bit of custom malware.
- A number of authorities are discussing supply-chain integrity concerns, in light of recent revelations of different government agencies tampering with computer equipment in transit between suppliers and customers. Part of that concern extends to cyber supply chains in the form of "cloud" products and services. Turbine vendors with their countless VPN connections deep into the heart of turbine control systems all over the continent are a kind of "cloud" vendor, as are comparable connections from other vendors.
- The recent Islamic State (IS) threats against the North American power grid are the first example of a credible terrorist threat to power systems. American Department of Homeland Security (DHS) authorities have described IS cyber attacks to date as "low capability" but have cautioned that the group has the money to purchase sophisticated attack capabilities.

4.10.2 Looking Forward

Looking forward, the French ANSSI standards paint the picture the most starkly. ANSSI permits only unimportant class 1 industrial control system networks, networks that are expendable to French society, to be managed according to standard IT best practices. More important class 2 and class 3 networks either should be, or must be protected by unidirectional gateways at perimeter connections to less-important networks.

No matter how expendable society regards an industrial process though, owners and operators of that process rarely regard their multi-million dollar investments as "unimportant" or "expendable." At this writing, many industrial process owners and operators have already deployed unidirectional protections, and many more have not. The key question owners and operators must ask looking forward is: which of our industrial control systems and industrial processes do we think are

expendable enough to our business, to be protected with only firewalls and other traditional IT protections?

Glossary and Acronyms

AD	Active Directory controllers store user names, passwords and permissions for Windows domains
ANSSI	Agence nationale de la sécurité des systèmes d'information—a French authority for cybersecurity
CD-ROM	Compact Disk Read-Only Memory—a widely-used optical disk format
CIP	Critical Infrastructure Protection—a set of NERC standards for cybersecurity in the North American electric grid
DDOS	Distributed denial of service—a type of cyber attack that uses large numbers of compromised machines to send messages or requests to a small set of targets, overloading the targets with messages and rendering them unable to respond to legitimate service requests
DHS	Department of Homeland Security—the American authority responsible for the American Cyber Emergency Response Team, Industrial Control System Cyber Emergency Response Team, and a number of other physical and cyber security programs
DMZ	Demilitarized zone—a network that lies "between" two networks at different level of trust
DNS	Domain Name Server—an Internet server that resolves human-readable domain names, such as "google.com" into IP addresses
DVD	Digital Versatile Disk—a widely-used optical disk format
EMS	Energy Management System—a control system that manages producers and consumers of electricity in a power grid
ENISA	European Union Agency for Network and Information Security—a European authority for cyber security
ERC	External Routable Connectivity—a legal definition in the NERC CIP Version 5 standards describing bi-directional, routable connectivity

FERC	Federal Energy Regulatory Commission—the American authority responsible for the reliable operation of the electric grid, and other energy infrastructures such as petrochemical pipelines
Firewall	A router with a filter, forwarding packets that pass the filter, and dropping or rejecting the remainder. Modern firewall filters can be complex, including signature-based and anomaly-based intrusion detection engines, in-line anti-virus scanners, and "deep packet inspection" engines
FLIP	A type of unidirectional gateway whose orientation can reverse on a schedule
ICCP	Inter-Control-Center Protocol—a communications protocol designed to communicate between control centers running EMS systems in a power grid
IDS	Intrusion Detection System—a cyber system designed to detect attacks on computers or networks, and raise alarms when such attacks are detected
IEC	International Electrotechnical Commission—an international standards and conformance body for all fields of electrotechnology
Inbound/outbound gateways	A pair of independent unidirectional gateway deployments, one replicating servers into a protected control system network, and one replicating servers out of that network
IP	Internet Protocol—the protocol used to communicate between hosts in the Internet
IPS	Intrusion prevention system—a cyber system designed to prevent attacks from compromising computers or networks
ISA	International society of automation—an organization working in the field of instrumentation, measurement and control of industrial processes
IS	Islamic State—a jihadist militant group
IT	Information technology—computers and networks deployed for conventional "business" purposes
NEI	Nuclear Energy Institute—an organization promoting the beneficial uses of nuclear energy
NERC	North American Electric Reliability Corporation—the organization mandated by FERC to design and enforce standards for reliability in the North American electric grid

NIST	National Institute of Standards and Technology—an American federal agency that develops technology standards
NRC	Nuclear Regulatory Commission—the American federal regulator for the safety of nuclear reactors and other civilian uses of nuclear materials
OT	Operations Technology—computers and networks deployed for industrial purposes
RX	Receive
TCP	Transmission control protocol—a workhorse protocol of the modern Internet, maintaining connections and packet delivery guarantees between IP endpoints
TX	Transmit
UDP	User Datagram Protocol—a workhorse protocol of the modern Internet, providing best-effort datagram service
Unidirectional Gateway	A hardware/software system that replicates industrial servers and emulates industrial devices through a hardware-enforced, unidirectional communications medium
USB	Universal serial bus—an industry standard for connection, communication and power supply between computers and electronic devices
VPN	Virtual Private Network—an encrypted extension of a private network across an untrusted network, such as the Internet
WAN	Wide-Area Network—a computer network extending over a large geographical distance

References

Ponemon Institute LLC. (2013) The Post Breach Boom.
Waterfall Security Solutions (2011) Introduction to Waterfall Unidirectional Security Gateways: True Unidirectionality, True Security.

Chapter 5
A Security Evaluation of a Municipal Computer Network: The Case of Collaboration Between the City of Pittsburgh and Carnegie Mellon University

Howard A. Stern

Abstract Since the decline of the steel industry, the City of Pittsburgh's reduced tax revenue has dramatically impacted its ability to provide essential municipal services, including an efficient and secure technology infrastructure. To overcome these budget shortfalls, the City has begun to explore partnerships with local universities. For example, the City's computer services department, in collaboration with a group of security students of the H. John Heinz III College at Carnegie Mellon University, undertook a comprehensive security evaluation of Pittsburgh's municipal computer network. The students identified numerous security breaches for the City while obtaining an invaluable real-world learning experience. This innovative collaboration can serve as a model for future government–university partnerships.

Acronym List

CCAC	Community College of Allegheny County
CenSCIR	Center for Sensed Critical Infrastructure Research
CIO	Chief Information Officer
CMU	Carnegie Mellon University
NDA	Non-disclosure agreement
SOX	Sarbanes-Oxley

H.A. Stern (✉)
School of Leadership and Social Change, Carlow University,
3333 Fifth Avenue, Pittsburgh, PA 15213 USA
e-mail: hastern@carlow.edu

R.M. Clark and S. Hakim (eds.), *Cyber-Physical Security*,
Protecting Critical Infrastructure 3, DOI 10.1007/978-3-319-32824-9_5

5.1 Introduction

Several years back, a prankster thought it would be amusing to replace the words "City of Pittsburgh" with a few choice obscenities in every outgoing real estate tax bill. Somehow, the intruder was able to penetrate the City's existing firewall and globally insert the off-color language without being detected by network administrators. Fortunately, an observant employee who was preparing the invoices for mailing discovered the offensive language and brought it to the attention of her supervisor who immediately halted distribution of the invoices.

Although Pittsburgh managed to avoid an embarrassing situation, questions arose as to how this intrusion could happen. In other words, how could a hacker penetrate the City's tax records and alter an invoice without anyone noticing? Furthermore, if a hacker could alter a tax bill, could one adjust an account to post a payment or overpayment? Finally, would it be possible to implement technical safeguards to prevent this and similar breaches in the future? Although the answers to these questions would not be easy, it had become apparent that a comprehensive information security audit and evaluation of the City's existing network infrastructure and policies was desperately needed.

Unfortunately, the City of Pittsburgh computer services department did not have the financial resources to undertake this evaluation. Faced with a diminishing budget and tremendous pressure to cut spending, the possibility of dedicating departmental resources to a professional security audit seemed unrealistic. As a result, the City's Chief Information Officer (CIO) decided to reach out to one of the City's academic partners, Carnegie Mellon University (CMU), to see if it would be interested in helping the City conduct a security audit of its computer network. This project would not only help the City obtain a much needed security assessment, but would provide the students with a "real world" experience.

5.2 The Creation of a Partnership

In the fall of 2008, The Center for Sensed Critical Infrastructure Research (CenSCIR) at CMU invited City of Pittsburgh government officials to meet with university faculty and administrators to gain a better understanding of the other's roles and responsibilities (Building a Productive Partnership 2001). The goal of this new initiative, called UniverCity Connections, "was to foster greater strategic and day-to-day communication and collaboration between the City of Pittsburgh and CMU, identify opportunities to cooperate on initiatives that are important to the City and the University, build relationships and lines of communication, and set the

stage for and build ongoing cooperation."[1] Through this collaboration, the City of Pittsburgh, a public agency and CMU, a nonprofit private organization, would complement each other by sharing unique resources of value to the other entity (Vernis et al. 2006).

During the inaugural meeting held at the CMU campus, City of Pittsburgh department heads were grouped by function and responsibility with CMU faculty and administrators. The City's Public Works director, for example, was paired with CMU's facilities management staff and faculty members who specialize in civil engineering. For technology initiatives, the City's CIO was paired with computer science and information systems faculty and staff. In the latter pairing, a flurry of discussions and ideas about possible collaborations ranging from shared disaster recovery services to joint software training were proposed. It soon became obvious that there were many issues of common interest for both CMU and the City. CMU was able to offer empirical research and resources from a diverse faculty while the City could offer a link between academia and the real world (Couto 2010a). The group suggested that the Associate Dean of Computer Sciences and the City's CIO serve as cochairs of this newly formed committee. Their function was to meet and discuss the group's priorities and agenda for possible future collaborations.

The newly appointed cochairs met around the time that Google announced its plan to build an ultrafast Internet connection in one or two American cities and that a competition for the best proposal would determine the winner. Realizing that a high-speed network could prove to be a boon for education, government, and health care, it became obvious that this initiative should be the committee's first priority. Within days of Google's announcement, both the City and CMU agreed to dedicate the appropriate resources to craft a unified proposal.

Although the Pittsburgh/CMU proposal was ultimately bested by that of Kansas City, the relationships formed during the application and planning process proved to be a catalyst for future collaborations, possible internships, and project opportunities for its public policy students. It was at this meeting that a security project of the City's network, to be conducted by CMU students under the direction of a security faculty member, was first proposed. This project was intended to assess and mitigate network vulnerabilities at the City of Pittsburgh. After the City submitted a detailed project proposal and schedule, the students and the faculty at The Heinz College overwhelmingly agreed to undertake this challenge.

[1]Center for Sensed Critical Infrastructure Research. (2008, December 18). *CenSCIR Plays a Role in Community Connections*. Retrieved from http://www.ices.cmu.edu/censcir/newsitem.asp?NewsID=585.

5.3 City of Pittsburgh Leveraging Its Resources

The Heinz College began to assemble a team of its best and brightest students with backgrounds in security, computer science, information technology, and public policy. Under the supervision of a CMU adjunct faculty member with extensive experience in cyber security, a group of five graduate students were selected to commence the fifteen-week, term-long study. In order to protect the confidential and sensitive nature of the project, both the supervising faculty sponsor as well as the participating students were required to complete and sign a non-disclosure agreement (NDA). The NDA would legally bar the graduate students from sharing or distributing any confidential or proprietary information, such as passwords or software vulnerabilities, to any persons not involved with the project.

5.4 The Students Begin

The students spent the first two weeks of the project trying to identify the vulnerabilities of the City's network by attempting to penetrate the City's firewall from outside its secure environment. The goal was to see if any of the applications or websites hosted by the City of Pittsburgh were susceptible to infiltration. The students applied easy-to-obtain software designed to scan for network weaknesses that would sniff, poke, and prod every publicly accessible site or application that the City makes available to the public. Ultimately, the students were successful in identifying a few sites that could be penetrated.

The next phase was to see if any network vulnerabilities existed within the organization itself. Realizing that an organization's own employees sometimes breach network security, the students decided to infiltrate the City workforce with the hope of identifying internal breaches. To uncover internal vulnerabilities, the City hired the students as City "employees." Unbeknownst to the City workforce, the CMU evaluation team was told to report to City offices under the guise of student interns who would be responsible for various municipal projects. With the exception of a few senior officials, no one knew the true nature of the students' work. After the standard employee orientation, the interns were deployed to City work locations with photo identification, work station space, logins, and permissions afforded only to new employees.

Similar to the external testing or initial phase of this project, the students once again deployed intrusion software in an attempt to break into the City's in-house systems. This time, however, the intrusion attempts were performed on those software applications that were only accessible to City employees who had permissions to access the in-house systems. The goal, of course, was to try and access password-protected computer systems that contained sensitive employee and taxpayer information, such as wage and employee records. While the student interns

had been issued student identifications and logins, they had not been given the passwords needed to (legitimately) access these sensitive records.

Fortunately, the newly hired interns had only limited success in penetrating the City's "in-house" systems through the standard technical intrusion techniques. Instead, the students decided to employ traditional social engineering techniques to trick people into volunteering confidential information, such as employee passwords. The idea was simple. Rather than use sophisticated software to extract personal information, why not simply ask the "keepers of the information" to provide access? Of course, managers would not just hand over data to any employee. Instead, a student called the organization's computer help desk, identified himself as a City employee, and explained that he had forgotten his password. The students were hoping that the technical help desk staff would simply provide passwords to the impersonators without proper verification. Happily, this technique was also unsuccessful. Following proper departmental protocol, the astute help desk technicians required additional authentication such as date of birth or last four digits of the employee's Social Security number before consenting to a password reset.

Since the students had no success in obtaining employee passwords by calling the help desk, the CMU interns decided to try a more sophisticated approach. The next approach involved the purchase and acquisition of email addresses that very closely resembled the standard email convention used by City employees: firstname.lastname@city.pittsburgh.pa.us. The students purchased email addresses that were identical except they deleted the period, between the words "city," "Pittsburgh," and "pa." (see Table 5.1).

Armed with these "imposter" email addresses in the names of high-level City officials (such as department directors), the CMU students issued an employee survey to a targeted group of workers. The goal, of course, was to persuade respondents to volunteer their credentials such as password or login name. In one trial, the students crafted an "Employee Satisfaction Survey" supposedly coming from the Human Resources director, requesting information about workforce attitudes toward employee benefits. As part of the survey, respondents were asked to log into the system by reentering their credentials into a Microsoft Outlook screen (see Fig. 5.1), similar to the one employees use each day. Once logged in, the employees' credentials and permissions were now captured. Most employees, seeing an email address that appeared to come from a City official, did not realize the survey was illegitimate. By changing the email address format ever so slightly and by employing the familiar Outlook login screen, the industrious students were able to fool many employees into voluntarily offering their passwords.

Within minutes of the survey's distribution, the real Human Resources director realized that a fictitious survey bearing her name had been disseminated to the City's workforce and promptly contacted the computer services department to halt

Table 5.1 Example email addresses for city employees

Legitimate email convention: John.Smith@city.pittsburgh.pa.us
Purchased (imposter) email address: John.Smith@citypittsburghpa.us

Fig. 5.1 Example employee satisfaction survey

its circulation. In response, the City's CIO, who did not initially know the students had initiated this bogus survey, blocked the disingenuous address and issued an immediate "all user" email, stating that the recent survey was fake and directing employees not to respond to it. The CIO further reminded employees that they should never volunteer their passwords to anyone, including their supervisor or the City's computer services department. The email added that employees that did surrender their passwords should immediately change them.

Of course, the student hackers did not care about the survey responses since it was the information from the completed Microsoft Outlook screen (see Fig. 5.1) that contained the user names and passwords that they wanted. Even though the survey was accessible for only sixty minutes, more than 15 % of respondents obliged, offering their personal log-in information. More surprisingly, many of the respondents who offered their credentials were senior-level officials.

5.5 Review of Policies and Procedures

The final phase of the security audit included a review of existing security policies and recommendations for new ones. In addition, the CMU students reviewed the City's existing policies to determine if they complied with federal statutory requirements contained in Sarbanes-Oxley (SOX) Act of 2002 and the Pennsylvania Right-to-Know law of 2009.

From an IT perspective, SOX requires organizations to retain company data, emails, electronic memos, e-files, and e-reports for a period of not less than 5 years. These requirements are designed to avoid conflicts of interest within an organization (Brehmer 2012). In addition, organizations are legally mandated to report security compromises or data breaches. To ensure compliance, the CMU students

examined the City's IT reporting systems and departmental policies and procedures. Their objectives were to make the City and its reporting methods more accountable, compliant, and transparent, in the event of an audit by the federal government (Wagner and Dittmar 2006).

The students also examined the City's existing policy on releasing public documents to ensure compliance with Pennsylvania's Right-to-Know law, which is overseen by the Commonwealth of Pennsylvania. Taking effect in 2009, this law posits that all government records are open and available to the general public unless the government agency can prove that any of the information is sensitive, confidential, or subject to exclusion under the law (Office of Open Records, Commonwealth of Pennsylvania 2014). To verify that the City's Right-to-Know policy was compliant, the CMU graduate students met with attorneys from the City's law department to review their understanding and interpretations of the Right-to-Know law and to help craft a policy that was both compliant and accommodating to the general public. As part of this policy, the students encouraged the City to post the names and telephone numbers on the City's website of those officials that could assist with Right-to-Know requests.

The graduate students also found that the City lacked a strong password policy. In some instances, the CMU students found that passwords for employee email accounts remained unchanged for months, even years. In collaboration with City staff, the students recommended a strong password policy. This newly developed policy, which was issued during the students' tenure at the City, required employees to craft a password that contains letters, numbers, and characters. The new password policy also required employees to change their passwords every six months. This policy was also extended to City-issued smart phones that provided employees with email access. Students pointed out that the loss of a Smart phone lacking password protection could prove to be an easy entry point into the City's network.

Finally, the students were asked to review and recommend changes to the City's existing electronic communications policy. This policy governed employees' use of computer equipment, Internet usage, and email access. Specifically, the policy made clear that any and all information stored on a City-issued computer or smart phone was the property of the City of Pittsburgh. It further advised that employees should have no expectations of privacy when it comes to online behavior engaged on a City computer or Smart phone. In the end, the students suggested that the electronic communications policy be revised to educate employees about proper usage of, and risks associated with, social media technologies such as Facebook or Twitter.

5.6 The Students Reveal the Vulnerabilities

Once the penetrations, social engineering, and policy reviews were complete, the students revealed their methods and phishing techniques to the City's technology staff. Intrigued by their ingenious tactics, the staff admitted that they had been aware of some unusual activity on the City's network. A City network and security

administrator commented that "at one point, we realized there was this 'cat and mouse' game going on and we didn't know where it was coming from. We were determined to stay one step ahead of these breaches." The graduate students reported that they performed scans of the City's servers, program applications, and websites to look for system vulnerabilities. Scans were used to identify open ports, improperly patched sites, and applications that were generally unsecured.

The students were successful in identifying several City websites and applications that contained improper permissions for user input. Additionally, many of these unsecured websites were running with administrative privileges that gave users the ability to access or modify the site. In other words, some City websites were allowing the employees to access data that they did not need. Often referred to as the "principle of least privilege," the students soon realized that some of the City's databases and websites gave users access to proprietary information that was unnecessary. For example, a public site developed to capture emergency contact information designed to notify users in the event of an emergency was found to contain permissions that allowed the CMU hackers easy access to the application database that stored the site's sensitive information. Instead of entering information, users were able to see the personal information of other site respondents.

As is often the case, once the students were successful in penetrating the emergency contact information website, they were then able to gain access to other sites that resided on the same host server. Thus, once a server is compromised, other sites on the same server become more susceptible to intrusions.

5.7 Lessons Learned

In the end, this unusual union helped both the CMU students and City technology staff gain a better understanding of the network infrastructure and the anti-intrusion software needed to combat future hacking. The students' findings allowed the City to take both a reactive and proactive approach to managing the data and integrity of its computer systems. In short, this understanding led to some immediate fixes and long-term security upgrades to make the City technology infrastructure a secure and safe environment.

In addition to the numerous policy and technical recommendations made by the students, there were three significant lessons that will serve as a launching pad for future collaborations. The first lesson is that partnerships between government agencies and academia can be successful when both sides benefit from the collaboration. The fact that the City of Pittsburgh got an expert review of its security infrastructure and CMU could offer its students a "real world" experience is proof that such partnerships do work. The challenge, however, is to get both entities talking and thinking "outside the box."

Perhaps the success of this project was due in part to the unique qualifications of the cochairs. The CMU representative was a faculty member who held an administrative position responsible for university-wide strategic programing and

initiatives. This position gave the CMU cochair unfettered access to faculty and administrators throughout the institution. Similarly, the City's CIO, with more than 25 years of municipal government experience, held a senior-level administrative position within local government with all the institutional knowledge and contacts afforded to that position. The City's CIO also had a terminal degree that allowed him to identify with his academic counterparts while being sensitive to the needs of a university. The champions are key for success in any partnership efforts for government entities.

The second lesson is that one successful project can lead to future projects. Within months of completing the security evaluation, the City and CMU spawned four new collaborative initiatives: (a) the development of a voice-activated spoken dialogue system for the City's nonemergency 311 operations center; (b) a joint grant application for the purchase of city-wide surveillance hardware and software; (c) a classroom project that measures the City's web-based traffic; and (d) the exploration of possible outsourcing of the City's computer services department. These projects were a direct outcome of the network infrastructure project.

Shortly after the security evaluation was completed, the CMU cochair introduced the City's CIO to a scientist at CMU's Language Technologies Institute, an office that researches and develops voice recognition software. Since the Institute had previously developed a bus scheduling system for the Port Authority of Allegheny County, the CMU cochair was hoping to use the same voice recognition technology to develop an application for the City. Within minutes of the introductory meeting, it became clear that another partnership was brewing. This time, the shared services team agreed to develop a spoken dialogue system for the City's 311 nonemergency telephone system that would handle road "pothole" complaints during nontraditional work hours. Instead of waiting for a live operator to handle the call, the automated voice recognition system would process and dispatch complaints when City 311 staff were not working. In other words, a citizen could report a "pothole" any time of the day or night and the call would be answered and dispatched immediately to a road crew that could investigate and patch the pothole immediately. In the past, the call would simply wait until the next business day.

After the proposed project was reviewed and agreed upon, a contract was prepared. Because this system involved the purchase and acquisition of hardware dedicated specifically to this project, the CIO agreed to provide a modest contribution from the City's operating budget.

Similar to the State of Oregon where joint grant applications between government and academia have led to strong collaborative partnerships (Fink 2011), the second collaboration was a $14 million joint City, CMU and Community College of Allegheny County (CCAC) grant application for the purchase of city-wide surveillance equipment and the development of a wireless network to store and index images. The money was available from a federal stimulus initiative for Broadband Technology Opportunities designed to enhance and expand the broadband infrastructure and Internet accessibility throughout the country (Smydo 2010). The City and CCAC sought these grant dollars to purchase additional cameras and CMU wanted to develop software that would analyze images and raw footage for

research applications. Both the City and its university partners felt that a joint application would strengthen their chances of submitting a successful application.

The third proposal spun off from the security evaluation was a classroom project that measured the network traffic of an organization's computer environment. The CMU professor who supervised the security project put the City's CIO in touch with a faculty member who was teaching a class on flow analysis, a protocol that monitors and identifies network traffic and patterns. Recognizing the potential benefits of a comprehensive evaluation of the City's network, the CIO agreed to participate in the study and release the City's traffic patterns to the class. From CMU's perspective, this collaboration would expand upon the in-class lessons and apply them to a real-world environment. In fact, the project and lessons learned from this experience were so successful that the faculty sponsor and CIO were invited to present their finding at FloCon, a national conference on computer network analysis and traffic.

A subsequent collaboration was the result of a conversation between the City's CIO and the faculty member who sponsored the security evaluation. As the CIO was expressing concern about the difficulties of recruiting and retaining qualified employees, it became apparent that a study evaluating the feasibility of outsourcing all or part of the City's computer services department would be a perfect project for another class. The CIO submitted a project proposal that was ultimately accepted by the College and its students. Under the direction of a faculty sponsor, a team of financial, technical, and public policy students was assembled to analyze the political and social issues of outsourcing the City's computer services department. As part of this study, the students examined budgets, evaluated technology alternatives, and identified the costs of the competing alternatives (Badertscher 2011). Similar to earlier collaborations, this project integrated classroom learning with real-world concerns and issues.

The final lesson learned from the initial security audit project is that collaborations save money. The cost of a professional network evaluation would probably have cost the City more than $100,000 had it hired a professional firm. By tapping the resources of one of its university partners, the City was able to benefit from this project at no cost to its taxpayer base. Given the current state of the economy, government officials and university leaders should encourage anenvironment of cooperation.

5.8 Conclusion

The City of Pittsburgh's partnership with the H. John Heinz College at CMU provided tangible and intangible benefits to both organizations. It saved the City money and protected scarce taxpayer dollars, while providing invaluable human capital and expertise. The CMU students gained real-world experience and the opportunity to put their education to the test.

Successful partnerships like this one tend to be contagious. The connections made and the ideas spawned have led to numerous conversations and additional collaborations. As demonstrated by the City/CMU security evaluation, collaborations are an effective tool for organizational power sharing that allows difficult problems to be confronted with creative solutions (Couto 2010b).

Fortunately, the synergy between the City and CMU continues and future partnerships are on the horizon. In the years since the UniverCity Connections' technology committee was formed, additional projects and partnership ideas have been proposed and implemented with the help of other local universities. Most importantly, the lessons learned in Pittsburgh can be replicated in other cities. Universities and governments alike must leverage their resources and become entrepreneurial if they are to continue to provide the same levels of service that their constituents and students demand, especially in such difficult economic times.

Acknowledgments I thank Philip Lehman, Timothy Shimeall, and Andy Wasser of Carnegie Mellon University for their invaluable help and support with the planning and execution of this six-month-long study. I also thank Alex Musicante, a systems security architect with the City Information Systems department of the City of Pittsburgh, for his invaluable advice. Finally, I thank Rhonda Wasserman, Professor of Law at the University of Pittsburgh School of Law, for her meticulous comments and suggestions, which have improved this book chapter immensely.

References

Badertscher, J. (2011, November 22). Graduate student of H. John Heinz III College at Carnegie Mellon University, Interview by author.

Brehmer, T. M. (2012, November). Sarbanes-Oxley has failed to address the problem of audit firm independence. *Accounting Today for the WebCPA*. Retrieved from http://www.accountingtoday.com/news/Sarbanes-Oxley-Failed-Address-Problem-Audit-Firm-Independence-64852-1.html

Building a Productive Partnership: A Meeting for Senior Executives from Community Colleges, Institutes of Technology and Federal Government Departments. (2001, September 25–26).

Couto, R. (2010a). *Political and civil leadership: A reference handbook*, Vol. 1. University of Minnesota, Sage Publications, Inc.

Couto, R. (2010b). *Political and civil leadership: A reference handbook*, Vol. 2. University of Minnesota, Sage Publications, Inc.

Fink, J. (2011, December 16). *Higher Education Universities' Research Collaboration Boosts Oregon*. Oregonian.

Office of Open Records, Commonwealth of Pennsylvania. Retrieved April 26, 2014 from http://openrecords.state.pa.us/portal/server.pt/community/open_records/4434

Plays a Role in Community Connections. 18 December 2003. Retrieved October 26, 2011 from http://www.ices.cmu.edu/censcir/newsitem.asp?NewsID=585

Smydo, J. (2010, April 2). *Pittsburgh calls for more cameras: Police say recordings led them to homicide suspects*. Pittsburgh Post-Gazette.

United States Security and Exchange Commission. (2002). Sarbanes-Oxley Act of 2002: Frequently asked questions. Retrieved from http://www.sec.gov/divisions/corpfin/faqs/soxact2002.htm

Vernis, A., Iglesias, M., Sanz, B., & Saz-Carranze, A. (2006). *Nonprofit organizations: Challenges and collaborations*. Palgrave Macmillia, St. Martin's Press.
Wagner, S., & Dittmar, L. (2006). *The unexpected benefits of Sarbanes-Oxley: Best practice*. Harvard Business Review, Retrieved May 12, 2014 from http://www.hbr.org

Chapter 6
Cyber Risks in the Marine Transportation System

Andrew E. Tucci

Abstract Since its earliest days, U.S. economic prosperity has been dependent upon maritime trade. The ships, boats, terminals, and related maritime critical infrastructure that support this trade are increasingly dependent on cyber technology. Cyber incidents involving navigation, cargo control, and other industrial processes could threaten lives, the environment, property, and could significantly disrupt regular trade activity. The U.S. Coast Guard, with long standing authority to address safety and security risks in the marine transportation system (MTS), encourages ship and vessel operators to establish a risk assessment and mitigation process to address cyber-related threats. State and local governments can contribute to this process through information sharing, and in Area Maritime Security Committees and other forums designed to address risk.

Acronyms

AMSC	Area Maritime Security Committee
CERT	Computer Emergency Response Team
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
GPS	Global Positioning System
IMO	International Maritime Organization
IT	Information Technology
MTS	Marine Transportation System
MTSA	Maritime Transportation Security Act
NIST	National Institute of Standards and Technology
SCADA	Supervisory Control and Data Acquisition
SOLAS	Safety of Life at Sea
USB	Universal Serial Bus

A.E. Tucci (✉)
United States Coast Guard, CG-FAC, 2703 Dr. Martin Luther King Jr. Avenue, SE, Mail Stop 75501, Washington, DC 20593-7501, USA
e-mail: Andrew.E.Tucci@uscg.mil

R.M. Clark and S. Hakim (eds.), *Cyber-Physical Security*,
Protecting Critical Infrastructure 3, DOI 10.1007/978-3-319-32824-9_6

6.1 Introduction

The marine transportation system (MTS) is an often overlooked component of the world's overall transportation and energy system, and the dominant factor in the global supply chain that connects businesses and individuals all over the world. By volume, over 90 % of U.S. overseas trade travels by water. Manufactured products, oil and natural gas, raw materials, and agricultural products move through U.S. ports every day. While these items are produced in many locations, they move via rail, truck, or pipeline into ports, where they are loaded onto ships and barges for export or further domestic transportation. The U.S. MTS includes approximately 360 major ports and over 8000 individual terminals along all of our coasts, the Great Lakes, and the Western Rivers—the Mississippi, Ohio, Missouri, and Columbia Rivers, plus their many tributaries. According to the U.S. Maritime Administration, waterborne cargo and associated activities contribute more than $649 billion to the U.S. GDP, sustaining more than 13 million jobs. Many thousands of vessels, from tugs and barges to ocean-going ships complete this system.

Box 6.1. US MTS Summary Statistics

U.S. Marine Transportation System

- 25,320 miles of navigable waterways
- 8240 marine terminals/facilities
- 9227 individual ocean going vessels made 79,091 port calls in the United States in 2014
- 12,100 passenger vessels (ferries etc)
- 12,175 tug and tow boats in the U.S.
- Waterborne cargo contributes more than $649 billion to the U.S. GDP

Box 6.1 contains some basic statistics regarding the US MTS. The MTS[1] and global supply chain are what enable construction equipment built in the U.S. heartland to be sold to companies in Europe and South America. It enables oil to be produced in the Gulf of Mexico, refined in Houston, and shipped as heating oil to New England. It sends grain from the Midwest down the Ohio and Mississippi Rivers to New Orleans and around the world. It brings everything from kiwi fruits to electronics to ore across oceans and the Great Lakes, up rivers, and into factories, retail stores, and homes.

World-wide, the MTS is making increasing use of cyber-dependent systems for a wide range of business and operational functions. Vessel and facility operators use

[1]American Association of Port Authorities. "Seaports and the U.S. Economy." http://aapa.files.cms-plus.com/PDFs/Awareness/US%20Economy%20Fact%20Sheet%2012-4-12.pdf. Accessed April 2015.

computers and cyber-dependent technologies for navigation, communications, engineering, cargo, ballast, safety, environmental control, and many other purposes. Computers control the temperature of refrigerated containers carrying food, medicine, and other temperature-dependent cargos. Emergency systems such as security monitoring, cameras, fire detection, and alarms increasingly rely on cyber technology. Ports use cyber systems to raise drawbridges, control traffic lights, schedule trucks to deliver and pick up containers, and use Supervisory Control and Data Acquisition (SCADA) systems to control pumps, valves, and pipelines delivering fuel and liquid cargo to ships.

Box 6.2. Effect of Panama Canal Expansion

The widening of the Panama Canal is accelerating port congestion trends on the U.S. East Coast. With ever larger ships calling at our ports, the need for speed and efficiency is all the more pressing. Cyber technology can help this situation—or hinder it if it is not managed properly. Efficient, resilient ports can promote local, regional, and global economic activity.

As in other business sectors, the marine industry uses cyber systems to facilitate financial transactions, execute contracts, place orders, and perform other business functions—often over wireless networks. The international aspect of marine transportation means that operators use cyber systems to provide ship, cargo, passenger, and crew information to customs officials around the world.

Collectively these technologies enable the MTS to operate with an impressive record of efficiency and reliability. While these cyber systems create benefits, they also introduce risk. Exploitation, misuse, or simple failure of cyber systems can cause injury or death, harm the marine environment, or disrupt vital trade activity. For example, vessels rely almost exclusively on networked geographic position systems (GPS) for navigation, while facilities often use the same technologies for cargo tracking and control. Each provides multiple sources of failure, either through a disruption to the GPS signal, or malware that impacts the way the signal is interpreted, displayed, and used on the vessel or facility.

Cyber vulnerabilities are in no way limited to GPS. Engineering and other systems are equally vulnerable. The US Coast Guard and other authorities have documented cyber-related impacts on technologies ranging from container terminal operations ashore to offshore platform stability and dynamic positioning systems for offshore supply vessels. While in some cases modern day pirates and smugglers have been the source of these events, others have been the result of nontargeted malware or relatively unsophisticated insider threats. Even legitimate functions, such as remotely driven software updates, could disable vital systems if done at the wrong time or under the wrong conditions.

Fig. 6.1 Typical control room on a modern passenger vessel. **Photo credit**: LCDR Eric Allen, U.S. Coast Guard

While high-profile events, often correctly described as deliberate attacks, grab most of the headlines, more mundane cyber events occur daily. Computers are as susceptible to poor programming, poor operation, and random error as any human-devised system. Indeed, from their earliest days, computers have been notorious for glitches and "bugs" (Fig. 6.1).

Commercial pressure and the ever-increasing demand for speed, efficiency, centralized control, and convenience create incentives to make greater and more integrated use of these systems. This in turn increases vulnerability and the "attack surface" available to hackers and criminals, as well as to simple misuse.

6.2 Computer Use in the MTS

While computers and computer problems are nothing new in society, or the maritime industry, two factors are increasing risks in the Maritime Transportation System. The first is that computers are now monitoring, supporting, or directly controlling virtually every aspect of marine operations. Mariners and port workers use, and rely on computers for everything from the top of the mast to the engine room, and from the front gate to the manifold at the end of the dock.

In the not so distant past, computers performed primarily business functions, or were a secondary support to operational activities. Now they are the primary, even sole controller of countless safety critical functions in the marine environment. That trend will only increase in the future.

The second factor is that these computers are networked with one another, and with computers around the world via the Internet. Even systems with no fixed Internet connection have periodic exposure via Universal Serial Bus (USB) drives and other interfaces. This connectivity, a hallmark of the twenty-first century economy, means that the attack surface vulnerable to malware rises exponentially

every time a new system is added, or upgraded to allow for remote monitoring or operation.

This combination of networked computers performing vital safety functions presents a serious challenge to the marine industry. We have always expected vessels to be sea worthy; now they must also be e-worthy. The "good marine practice" that vessels and marine terminals have adopted now must include good cyber practice. Cyber checks need to be part of the routine procedures vessel and facility operators undertake to ensure day-to-day safety.

We have already seen cyber impacts to vessels and port facilities, here in the United States and abroad. For example, the U. S. Coast Guard has noted with concern several instances in which malware impacted the dynamic positioning systems used for precise navigation control in the offshore oil industry. These operations, which involve large ships maneuvering alongside oil rigs in an offshore environment, are potentially dangerous. In one instance, investigators linked a sudden, unexpected power loss to viruses found on the software controlling the system. Thankfully there were no injuries, damage, or pollution but the potential for such consequences is clear.[2]

In another navigation incident, a crew member plugged his smart phone into a ship's electronic chart system to charge the phone's battery. Malware on the phone migrated to the system and deleted or corrupted all of the charts, causing a two-day delay in the ship's schedule while technicians restored the system.[3]

The above instances are best described as cyber accidents rather than attacks—there was no deliberate intent, just poor cyber practices that allowed malware to impact safety critical systems. Had the events been targeted, they might have occurred at the worst possible times and resulted in serious consequences.

Port facilities are also vulnerable to attack and accident. In one well-publicized incident, organized crime exploited a European container terminal's cargo tracking system to facilitate drug smuggling. They penetrated and exploited the system to track the cargo containers that included the narcotics and schedule their pickups.[4] Transnational organized crime has also used cyber technology to facilitate the sale of stolen cargo, and for other financial gains in the shipping industry.[5] The large sums used by the shipping community, in combination with the wide assortment of agents, cargo owners, suppliers, and other business partners with whom they must interact make shipping an inviting target for cybercrimes.

[2]U.S. Coast Guard investigations 2011–2015, and personal communications by the author.

[3]Coast Guard Field Intelligence Report dated 27 July 2015 (For Official Use Only).

[4]Europol Public Information Intelligence Notification 004-2013, European Cybercrime Center.

[5]See for example, "oil and gas industry targeted by hackers", last accessed 8 February 2015 at http://securityaffairs.co/wordpress/36843/cyber-crime/cyberattacks-on-oil-and-gas-firms.html.

Fig. 6.2 Coast Guard personnel observing the security and safety control systems at a marine terminal. USCG photo

6.3 The U.S. Coast Guard Strategic Approach

The Coast Guard's operating model for all types of risk is to prevent incidents, accidents, and attacks whenever possible, and to be prepared to respond to those events when they do occur. Both have a role in the Coast Guard's Cyber Strategy. In Appendix A, the cyber risk "bowtie model," illustrates some of the prevention and response-related aspects of this approach (Wierenga et al. 2009; Khakzad et al. 2012).[6]

The prevention side of this equation is to identify and establish broadly accepted industry standards that reduce the likelihood of an incident occurring. In developing prevention standards and programs for cyber and other vulnerabilities, the following principles apply (Fig. 6.2).

6.3.1 Principles of the Coast Guard's Prevention Program

The Coast Guard's prevention standards are ***risk based***. That is, they correlate the degree of protection with the potential consequences. For example, vessels and facilities that handle liquefied natural gas are subject to greater requirements than those that handle most other products. For any individual vessel or facility, vital

[6] www.cgerisk.com, last accessed 4 March, 2016.

systems such as firefighting, lifesaving, and communications are generally given more scrutiny than those with only a secondary influence on safety or security.[7]

In addressing potential cyber vulnerabilities, the Coast Guard is following a similar risk-based approach. While a vessel or facility may have any number of cyber-dependent systems, our concern is with those few where failure or exploitation of the system might result in significant safety, security, or environmental consequences.

A second principle is that the Coast Guard uses ***performance standards*** wherever possible. That is, the purpose of our standards is to achieve a high degree of safety and security performance—to protect the mariners, facility workers, and vessel passengers from harm, to protect the marine environment, and to avoid damage to property and equipment.[8] There are many ways to accomplish that goal, and the Coast Guard strives to allow industry the greatest flexibility. In some cases, such as with our Maritime Transportation Security Act requirements, our regulations are almost entirely performance based. Even in cases where more prescriptive requirements are appropriate, such as engineering standards, the Coast Guard allows and encourages industry to propose alternative methods that achieve an equivalent level of safety or security.

Despite the technical nature of cyber systems, the Coast Guard believes that the principle of performance standards can and should be part of any vessel or facility's approach to reducing cyber risks.[9] In some cases, an operator may choose to mitigate a cyber vulnerability through an established technical protocol. In other cases, training programs, physical access controls, or a simple manual backup may be a better option. The business needs of the organization should serve to identify the best method of reducing the risk. A third aspect of the Coast Guard's Prevention model is that our standards reflect the ***unique risks of the marine environment.***[10] Heat, vibration, salt water, weather, and other factors require standards suitable for this environment. Coast Guard approval of items such as extinguishers and marine wiring reflects this reality.

The marine environment includes unique risks that any cyber risk management effort must address. These include serious consequences to people, the environment, property, and the MTS as a whole. The Coast Guard's cyber risk management program is concerned with these special maritime risks. Businesses certainly face other cyber risks, such as the loss of proprietary or financial data.

---

[7]See for example 33 Code of Federal Regulations Part 127, which details requirements for liquefied natural gas facilities.

[8]U.S. Coast Guard Marine Safety Manual, Volume 1, Administration and Management, COMDTINST M16000.6, chapter 1, available at https://www.uscg.mil/directives/cim/16000-16999/CIM_16000_6.pdf.

[9]For example, 33 Code of Federal Regulations Part 105.260(a)(6) requires waterfront facilities to protect security and surveillance equipment, but does not specify *how* that must be done.

[10]U.S. Coast Guard Marine Safety Manual, Volume 2, COMDTINST 16000.7B, Chapter 1 describes marine equipment and materials. Available at https://www.uscg.mil/directives/cim/16000-16999/CIM_16000_7B.pdf.

These risks, while very real, are not unique to the maritime environment and are outside the Coast Guard's mission. The technical aspects of cyber security are also not uniquely maritime. Computers onboard a vessel or on a marine facility are no different from those in other environments, and the threats they face come in one and zeros wherever the computer is located and without regard to its ultimate function. Technical protocols need to be appropriate for the system and threat in question. They need no modification for vessel or marine facility use.

6.3.2 Response, Investigation, and Recovery

Because we cannot expect to prevent all incidents (cyber related or otherwise), preparedness is equally important to reducing the overall risk to the public and MTS. In many cases, addressing the consequences of a cyber event—such as an oil spill caused by computer controlled pump—is no different than if the incident had no cyber aspect. In such an incident, the responsible party would activate their spill response plan under the direction of the Coast Guard and other agency officials.

The Coast Guard investigates pollution incidents, marine casualties, and certain other incidents to determine the factors that led to the incident and prevent reoccurrences. If the investigation reveals a cyber nexus, the Coast Guard will work with law enforcement and other appropriate agencies to gather evidence and support criminal prosecution. In all cases, the Coast Guard will typically require the operator to conduct tests or inspections to ensure a system is safe before resuming normal operations. For cyber incidents, that process might include measures to ensure a system is free of malware or known vulnerabilities.

6.3.3 How Can Vessel and Facility Operators Manage Cyber Risks?

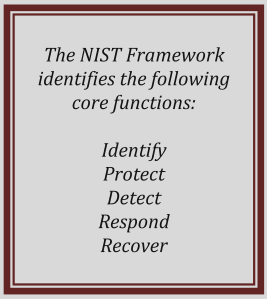
The marine industry has a long history of success in risk management. Mariners and port workers identify and evaluate risks on every watch and shift. Vessel and facility operators should view cyber along with the physical, human factor, and other risks they already face. The National Institute of Standards and Technology (NIST) published the NIST Framework, which provides guidance on how to accomplish this.[11] The first step is to identify and evaluate the sources of risk. While physical and personnel risks are relatively easy to identify, cyber risks pose a unique challenge. Cyber vulnerabilities are invisible to the casual observer and cyber-attacks can originate from anywhere in the world. Information technology

[11] http://www.nist.gov/cyberframework/.

specialists can help, but their focus is often with routine business applications. Information Technology (IT) specialists may not fully recognize.

Box 6.3. NIST Framework

The various operational systems on a vessel or waterfront, the potential consequences should they fail, or have an operator's perspective on potential nontechnical (and lower cost) solutions.



6.3.3.1 Risk Assessment

To assess cyber risk, designate a responsible individual and assemble a team that includes operators, emergency managers, safety, security, and information technology specialists.[12] Very briefly, their risk assessment process would proceed as follows:

- Inventory cyber-dependent systems that perform or support vital operational, safety, security, or environmental protection functions.
- Map any connections between these systems and other networks. Note which systems are accessible via routine Internet connection and for portable media such as USB and CD drives. This step in the process helps to identify potential **vulnerabilities**. Note that even systems with no connection to the Internet whatsoever are still subject to insider threats and simple technical failures.
- For each system, discuss the potential **consequences** if the system was exploited, malfunctioned, was unavailable, or simply failed under "worst case scenario" situations. Remember, Murphy's Law always applies, and adversaries may combine a cyber attack with a physical attack.
- Considering both the vulnerability and the potential consequences, evaluate the relative risk for each system. Systems with multiple vulnerabilities and

[12]A holistic view of risks and solutions is arguably the most important step.

high-potential consequences have higher risk than those with few vulnerabilities and low-potential consequences.

6.3.3.2 Risk Mitigation

Once the team recognizes their cyber risks, the organization can select mitigation strategies to reduce that risk. Prevention/protection strategies reduce vulnerabilities and the frequency of successful attacks or adverse events. While high-risk systems should naturally have more robust protection strategies, this does not necessarily equate to sophisticated technical solutions. For example, physical access control and training may be sufficient for systems where the primary vulnerability is an insider threat. Where risk managers choose technical solutions, they must also recognize their limitations.

Many systems are only capable of recognizing and blocking known threats. Unfortunately, the pace of innovation in the malware world is increasing, zero day exploits are common, and a strategy that relies exclusively on a perimeter defense designed to filter out known threats will not be successful.

Operators can also reduce risk at the consequence end. For example, manual backups may be appropriate for situations where the cyber failure is disruptive, but does not include immediate life, safety, or environmental impacts. Manual backups can be an excellent way of building cyber resilience—provided the old fashioned manual system is reliable and personnel still know how to use it!

Exercises can help identify the procedures an organization may need to take to isolate a suspect system, purge it of malware, and safely resume operations. Including a cyber aspect into an existing security, natural disaster, or environmental response plan can help an organization prepare for a cyber incident with an "all hazards" approach.

The teamwork approach among operators, IT specialists, and other risk managers is vital. Only a multitalented team can develop multitalented solutions. Regardless of the strategy chosen, operators need to see risk assessment and risk mitigation as continuous processes, not one-time events. While this is true for any risk an organization may face, the rapid change in technology and its ever increasing use in society make this especially important.

Box 6.4. Definition of Defense in Depth

The term *Defense in Depth* refers to a multifaceted and multilayered approach to cyber defense. Defense in depth considers the various people, technology, and operating policies an organization might adopt. It includes protection, detection, response, and recovery activities. Defense in depth recognizes that no single strategy can ensure security.

6.3.3.3 Risk Management

Once an organization has identified, evaluated, and mitigated cyber-related risks to an acceptable level, it must still do two things to maintain that condition. First, organizations need to incorporate their cyber procedures into appropriate internal policy and operating requirements. These will vary from organization to organization, but may include the following:

- Safety Management System/ISO procedures
- MTSA required security plans
- Operations manuals
- Continuity of Operations/Continuity of Business plans
- Company training programs and policies

Second, because no risk is static, organizations must view cyber security as a process, and establish a regular schedule to review cyber risks, reevaluate the need for mitigation measures, and ensure personnel understand and can follow good cyber practices. Rapid changes in technology and ubiquitous cyber threats make this concept especially important. Ultimately, an organization should strive to incorporate cyber into an existing culture of safety, security, and risk management.

Cyber risk management is a leadership responsibility. Organizations should identify a senior individual as the person responsible for cyber risk management. That individual, and other leaders, must recognize that creating a strong cyber culture as an "all hands" responsibility. With the visible backing of senior leadership, an organization can develop the strong cyber culture needed to keep the operations safe, secure, and efficient.

6.3.4 Information Sharing

Information sharing is a vital component of cyber risk management, and has benefits in both preventing incidents, and managing them when they do occur. Information sharing among industry peers, and with government agencies, can allow a company to identify possible vulnerabilities in their systems, anticipate attacks, and provide access to software patches and other mitigation tools. Some reports indicate that as much as 85 % of successful cyber breaches are in part preventable in that they exploit known vulnerabilities for which software patches have been available for at least a year.[13]

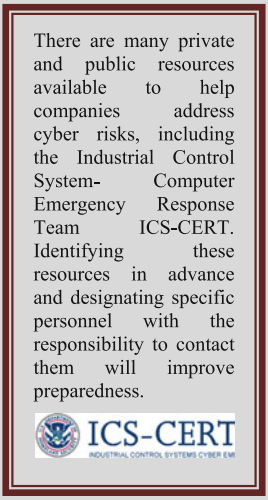
Of course information sharing can also be useful after an incident. "Zero Day Attacks" are attacks that exploit previously unknown vulnerabilities. Reporting these incidents can help spread the word to others and enable them to prepare.

[13]US-CERT, Top 30 Targeted High Risk Vulnerabilities, https://www.us-cert.gov/ncas/alerts/TA15-119A, accessed 8 February 2016.

Reporting incidents to trade associations, regulators, and others may also provide access to mitigation measures.

Reporting to law enforcement and government agencies is required in some industries, and can help public servants "connect the dots" if there is a pattern to attacks that suggests further attacks (including physical attacks) are likely, or can help authorities identify the perpetrators.

Box 6.5. NIST Framework



Commercial vessels and facilities subject to the Coast Guard's Maritime Transportation Security Act regulations must report suspicious activity, breaches of security, and Transportation Security Incidents to the U.S. Coast Guard. This includes incidents and activities with a cyber nexus. The Coast Guard works with the Computer Emergency Response Team (CERT) and other entities to investigate these reports.[14] To better understand cyber and other threats, the U.S. Coast Guard maintains regular communications with a wide range of government, industry, and academic organizations. As a member of the United States Armed Forces, the Coast Guard operates in the .mil domain, and supports U.S. CYBERCOM[15] in defending the nation from attack. As a component of the Department of Homeland Security, the Coast Guard operates in the .gov domain, and maintains a liaison officer at the National Cybersecurity and Communications Integration Center. The Coast Guard cooperates with many other government agencies including the Environmental Protection Agency, the Department of Energy, and the National Oceanic and

[14]The U.S. Coast Guard maintains a liaison officer at the National Cybersecurity Communications and Integration Center (NCCIC) to facilitate interagency cooperation.

[15]U.S. Cyber Command is an armed forces unified command that centralizes command of cyberspace operations and defense of U.S. military networks.

Atmospheric Administration. Through the Coast Guard Academy in New London, CT, the Coast Guard operates in the .edu domain, and cooperates with other academic institutions on cyber security research. Finally, the Coast Guard works extensively with the private sector, including shipping companies, port operators, and related industry associations. Information sharing across all of these segments of society is a challenge not because of any unwillingness to cooperate, but simply due to the volume of information, the myriad of threats, and the limited budgets of all the organizations. Appendix B summarizes the roles and responsibilities for the various US Agencies involved in cyber security.[16]

6.3.4.1 State and Local Involvement

While the MTS is part of the global supply chain, state and local involvement in cyber risk management is absolutely essential. Ships and port facilities connect to and rely on state and locally controlled critical infrastructure, such as power grids, potable water, and waste disposal, and telecommunications, for routine operations. Bridges and roads are owned and operated by states or municipalities. The traffic lights, draw bridges, and the cameras and sensors they use for safe and efficient operation are increasingly controlled by cyber-dependent systems. Maritime stakeholders and state and local governments therefore have a shared responsibility and shared interest in cyber risk management.

Area Maritime Security Committees are an ideal venue for cooperating across jurisdictional lines. These port-level organizations are chaired by the local Coast Guard Captain of the Port and include representatives from private industry, and from federal, tribal, state, and local government. They are responsible for addressing security concerns including those related to cyber incidents.[17] Local Emergency Planning Committees and other local and regional preparedness organizations should consider how they will respond to a significant cyber disruption of marine and other transportation-related critical infrastructure.

6.4 Ongoing and Future Coast Guard Cyber Activity

The U.S. Coast Guard is working to develop the skills, policies, and programs that we will need to address cyber risks. In 2012, we directed all of our Area Maritime Security Committees (AMSC) to consider cyber alongside more conventional risks

[16]A full description of all U.S. government cyber authorities is beyond the scope of this paper. See for example, "Cybersecurity, National Strategies, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented, GAO-13-187, and http://www.dhs.gov/topic/cybersecurity.

[17]Title 33, Code of Federal Regulations, Part 103.405 address AMSC responsibilities, including computer systems and networks.

as they evaluated potential security risks to their ports.[18] Established by the Maritime Transportation Security Act, AMSCs are public–private partnerships, chaired by the local Captain of the Port. They include representatives from the federal, state, and local government, private industry, labor, and other port stakeholders.

Across the country, AMSCs have established cyber subcommittees, evaluated cyber security risks, held cyber-related exercises, and assisted in the evaluation of port security grant funding, including grants directed specifically at cyber security vulnerabilities. AMSCs also serve as a forum to share best practices across government and industry, such as the FBI's InfraGard program.[19]

The Coast Guard is also working in partnership with various groups to evaluate and address cyber risks more systematically. Working with the American Association of Port Authorities and the National Institute of Science and Technology, the service is developing a cyber risk profile for bulk liquid terminals—such as those that transfer oil, gasoline, and liquid hazardous materials. Given the potential consequences of, for example, a sudden release of toxic materials in a populated port area, this is an area of primary focus.

Much of the Coast Guard's work involves collaboration with experts in government, industry, and academia. The Department of Energy's (DOE) Cyber Capability Maturity Model is potentially useful for the marine industry. The DOE also has extensive experience in protecting the nation's power grid from attack. To better understand risks and prepare for the future, the Coast Guard has sponsored cyber seminars and workshops at Rutgers University, the Coast Guard Academy, and most recently at the California Maritime Academy. Because cyber is an inherently international issue, the Coast Guard is working closely with Canada, other nations, and at the International Maritime Organization, to address cyber risks.

As technology continues to progress, the need to address the associated cyber risks will only grow. Real-time monitoring of engine performance and other processes, along with increasingly sophisticated navigation and information system are driving the need for cyber reliability. So is automation—robot ships with no crew whatsoever are now on the drawing board and will soon be a reality. Insurers, investors, customers, and public servants are creating pressure for the operators of these systems to demonstrate their safety. Big data, smart sensors, software developments standards, there is no cyber silver bullet, nor will any collection of methods ever completely eliminate cyber risks. What we can and must do is to work together to understand and manage those risks to an acceptable level. Appendix C contains a hypothetical but hopeful case study that illustrates the positive potential of effective marine cyber security.

[18]U.S. Coast Guard Navigation and Inspection Circular 09-02, Change 4, Enclosure 3. Available at www.uscg.mil/hq/cg5/nvic.

[19]http://www.infragardmembers.org/.

6.5 Summary and Conclusion

The U.S. Coast Guard is proud of its service to the country. The Coast Guard is also grateful for the professionalism and cooperation of the marine industry in helping to build and operate the safest, most secure MTS in the world. The ports, terminals, vessels, locks, dams, bridges, related infrastructure and, most importantly the people that operate it drive the American economy and are vital to the nation's strength and prosperity.

Despite the apparent complexity and scale of cyber threats, cyber has been added to a long list of risks the maritime industry and the Coast Guard have overcome. More senior members of the Coast Guard and of industry can look back on their careers and see great advances in environmental stewardship, safety, and conventional security. Those accomplishments reflect a cooperative approach that establishes meaningful standards to address real risks, devises flexible strategies to meet those standards, and shares responsibilities to maintain those systems over time. The nation has been strengthened and the Coast Guard and the Maritime industry have ensured that our ports and waterways are a safe place to live, conduct business, and link our economy to the world.

While cyber risk management certainly requires some technical skills from the current and next generation of leaders, it will succeed on the foundation of those of us (this author included) that still think an A-60 bulkhead[20] is the best firewall for any situation.

Appendix A—Cyber Risk Bowtie Model

The model below depicts cyber risk management activities. On the left, the model notes several types of attack or threat vectors. These range from sophisticated, targeted attacks from "Advanced Persistent Threats" (including, but not limited to nation-states), down to a simple technical error, such as improper software updates. The term "insider threats" also represents a broad range of actors—from those with special access and a desire to inflict deliberate harm on an organization to those who unknowingly introduce malware by clicking on the wrong link or plugging a personal smart phone or other device into a USB drive or other port (Fig. 6.3).

Prevention/Protection measures reduce the likelihood of an incident by creating barriers to the malware or other measures that can compromise a system. These include technical measures, policy and training, and physical access controls. Once an incident has occurred, communications, response, and contingency plans reduce the impact of the event and promote rapid recovery. An organization with

[20]An A-60 bulkhead is a structural fire protection standard for ship construction. It refers to the ability of a bulkhead to prevent the spread of fire and smoke for 60 min.

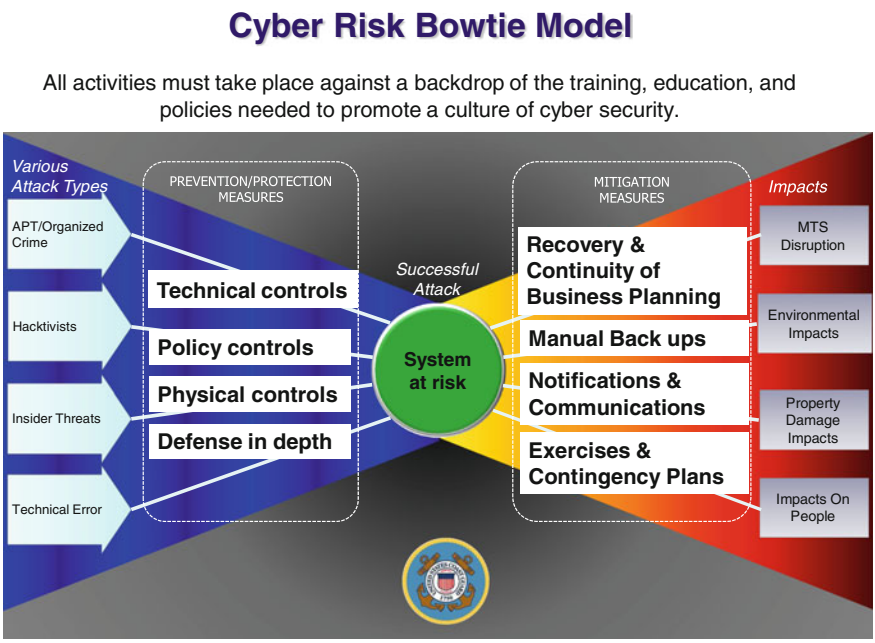


Fig. 6.3 Schematic illustrating the Cyber Risk Bowtie Model

strong cyber resilience will consider all types of threats, institute both protection and response procedures to reduce risk, and promote a strong culture of cyber security through training, education, and leadership.

Appendix B—Cyber security Roles and Responsibilities

A full discussion of the various cyber security-related authorities and responsibilities within the federal government is beyond the scope of this paper. Broadly speaking, the Department of Homeland Security is primarily responsible for critical infrastructure protection, the Department of Justice is primarily responsible for criminal investigations, while the Department of Defense is responsible for national defense (Table 6.1).

These descriptions are best understood as generalizations. Individual agencies often have their own, unique authorities. For example, within DHS, the U.S. Secret Service has authority to investigate and prosecute certain types of computer fraud and other cyber crimes.

The U.S. Coast Guard, as a member of the Department of Homeland Security, has responsibility to help protect the nation's maritime critical infrastructure, and to promote safety and security in the MTS. As a member of the U.S. Armed Forces,

Table 6.1 Summary of roles and responsibilities for US agencies involved in cyber security

	DHS	DOJ	DOD
Lead role	Protection, information sharing	Investigation and prosecution	National defense
Responsibilities	Coordinate national response to significant cyber incidents Disseminate domestic cyber threat and vulnerability analysis Protect critical infrastructure Secure federal civilian systems Investigate cyber crimes under DHS jurisdiction Coordinate cyber threat investigations	Prosecute cyber crimes Investigate cyber crimes Lead domestic national security operations Conduct domestic collection and analysis of cyber threat intelligence Coordinate cyber threat investigations	Defend the nation from attack Gather foreign cyber threat intelligence Secure national security and military systems Support the national protection, prevention, mitigation of, and recovery from cyber incidents Investigate cyber crimes under military jurisdiction

the Coast Guard works closely with the Department of Defense, including U.S. Cyber Command, in defending the nation. As a law enforcement agency, the Coast Guard has authority to investigate violations of all federal crimes with a maritime nexus (14 U.S.C.). Finally, the Coast Guard is a member of the intelligence community, providing us access to many sources of information that can help us with our mission to protect the American people.

Appendix C—A Cyber Safe Port: A Hypothetical But Hopeful Case Study

As an oil tanker approaches the coast, the Electronic Chart Display and Information System records the ship's GPS position and automatically signals the engine room to switch to the clean burning fuels required to meet air quality standards for nearshore navigation. The crew on the bridge and in the engine room confirm the signal and monitor the Engine Management System as it controls the sequence of valves and pumps needed to make the switch correctly. The system also sends a report to state authorities and the ship's owners, including sensor data confirming proper operation.

Thanks to the ability to securely download the latest charts and navigation information while still at sea, the crew and local pilot have the most up to date and

accurate information about currents, channel depths, and aids to navigation. The ship enters the harbor safely.

Inside the harbor, the ship approaches a drawbridge that carries thousands of cars and trucks each day. Cyber systems raise the bridge, and have already sent alerts to drivers on the road, minimizing the impact on traffic. The tanker transits through the bridge. Computer-controlled systems on the ship, and on the assisting tug boats, control the engines and rudders, helping the mariners tie up the ship with precision and safety. Cyber systems on the ship, and on the terminal, help manage the transfer of gasoline, heating oil, and aviation fuel from ship to shore. Cyber systems on the terminal control the valves and pumps that distribute the different products to the appropriate storage tanks, providing real-time information on tank levels, product flows, environmental monitoring, and other information needed to run a safe and efficient business.

Meanwhile, a container ship approaches another terminal in the port. Although the ship will unload and load thousands of individual shipping containers, truckers and the terminal have devised a web-based system to schedule individual pickups, avoiding the long backups that previously clogged the local roads. Fully automated systems move the containers from the ship to the waiting trucks. Perishable goods and materials needed for just-in-time manufacturing make it to their destinations on time. Other cyber systems track the exact location of cargo waiting at the terminal to be loaded for export, including hazardous materials. Biometric identification cards are part of the access control system for the facility, as are computer controlled cameras, gates, and communication systems. The tracking and monitoring functions include state-of-the-art authentication and other security features, so that emergency responders, law enforcement agencies, and cargo owners have the information they need while denying criminals and others without a legitimate need to know.

The secure, efficient systems make the port a top choice among shippers. Vessel and facility operators diligently install required software updates, train crew, and employees on good cyber practices, and share information on emerging threats and vulnerabilities. These practices, combined with clear documentation, keep auditors happy and insurance premiums low.

In the Port Authority building, members of the Area Maritime Security Committee are meeting to plan their next security assessment and exercise. The Committee members include the Coast Guard, the FBI, Customs, state and local agencies, and many representatives from the private sector. They consider cyber along with other security risks, and develop contingency plans, conduct exercises, and share lessons learned. The Committee recognizes that despite their best efforts, successful cyber-attacks or simple technical failures at some point are likely. Their plans therefore include manual backups, notification procedures, and recovery plans to minimize the impact of those events. These plans, and the cooperative spirit in which they are made, improve the regions resilience for cyber and other hazards.

The above scenario is hypothetical only in that the technologies described are not widely adopted. Wise cyber risk management practices can help ensure that safety and security go hand in hand with technology.

References

Khakzad, N., Khan, F., & Amyotte, P. (2012). Dynamic risk analysis using bow-tie approach. Reliability Engineering and System Safety, *104,* 36–44.

Wierenga, P. C., Lie-A-Huen, L., de Rooij, S. E., Klazinga, N. S., Guchelaar, H.-J., & Smorenburg, S. M. (2009). Application of the Bow-Tie model in medication safety risk analysis. *Drug Safety, 32*(8), 663–673.

Chapter 7
Creating a Cyber Security Culture for Your Water/Waste Water Utility

Srinivas Panguluri, Trent D. Nelson and Richard P. Wyman

Abstract Water is a vital resource. In the Water Sector, the U.S. Environmental Protection Agency (EPA) is the lead agency for protecting the critical infrastructure. The EPA has determined that a voluntary approach to cyber security is sufficient for protecting critical infrastructure in this sector. Also, the EPA is in collaborative partnership with the Department of Homeland Security (DHS) to ensure cyber security in this sector. In 2014, the DHS responded to 14 cyber security incidents reported by the Water Sector. The established techniques of cyber-attacks are documented in this chapter along with a summary of common vulnerabilities. A sector-specific example of a secure-network design architecture is presented and discussed in this chapter. However, the variability of organizational size and availability of resources in this sector makes a template technological approach difficult to implement. While understanding the technological approaches including hacking tools and defense in depth are important countermeasure mechanisms, a cultural approach is necessary to control the human element which makes the selected technological approach a viable measure.

Acronyms/Definitions

AAL	Advanced Analytical Laboratory
AD	Active Directory
ANSI	American National Standards Institute
APT	Advanced Persistent Threats
AWWA	American Water Works Association
BGD	Billion Gallons per day

S. Panguluri (✉)
CB&I Federal Services LLC, 5050 Section Avenue, Cincinnati, OH 45212, USA
e-mail: Srinivas.Panguluri@cbifederalservices.com

T.D. Nelson · R.P. Wyman
Cybersecurity Consultant, Idaho Falls, ID, USA
e-mail: Trentn@cableone.net

R.P. Wyman
e-mail: rwyman.cse@gmail.com

R.M. Clark and S. Hakim (eds.), *Cyber-Physical Security*,
Protecting Critical Infrastructure 3, DOI 10.1007/978-3-319-32824-9_7

C	Consequence
C3	Critical-Infrastructure Cyber Community
CDs	Compact Disks
CSET	Cyber Security Evaluation Tool
CWA	Clean Water Act
DHS	Department of Homeland Security
DLLs	Device Link Libraries
DMZ	De-Militarized Zone
DoS	Denial of Service
DVD	Digital Video Disk
EO	Executive Order
EPA	U.S. Environmental Protection Agency
FTE	Full-Time-Equivalent
HSPD	Homeland Security Presidential Directive
ICS	Industrial Control Systems
ICS-CERT	Industrial Control System Cyber Emergency Response Team
IDS	Intrusion detection systems
IP	Internet Protocol
IPSEC	Internet Protocol Security
MAC	Media Access Card
MGD	Million Gallons per day
MIM	Man-in-the-middle Attack
MITM	Same as MIM
MLD	Million liters per day
NCCIC	National Cybersecurity and Communications Integration Center
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
Nmap	Network Mapper
NVD	National Vulnerability Database
O&M	Operations & Maintenance
OSINT	Open-Source Intelligence
OS	Operating System
PLCs	Programmable Logic Controllers
POTW	Publicly Owned Treatment Works
PPD	Presidential Policy Directive
PWS	Public Water Systems
RTUs	Remote Terminal Units
SCADA	Supervisory Control and Data Acquisition
SDWA	Safe Drinking Water Act
SIEM	Security Information and Event Management
SQL	Sequential Query Language
T	Threat
TLD	Trillion liters per day
USB	Universal Serial Bus

USCERT	United States Computer Emergency Readiness Team
V	Vulnerability
VLANs	Virtual Local Area Networks
VPN	Virtual Private Networks
WAN	Wide Area Network
WRF	Water Research Foundation
WERF	Water Environment Research Foundation

7.1 Introduction

Water is a vital component of human life, and access to safe drinking water is essential for human survival. After water is used, the resulting wastewater must be treated to prevent disease and damage to the environment. From a public health and an economic perceptive, both water and wastewater utilities represent critical infrastructures that must be protected. The terrorist attacks of September 11, 2001, brought to light the many threats and vulnerabilities faced by the United States. In response, the federal government directed efforts to secure the nation's critical infrastructure and initiated programs such as the National Strategy to Secure Cyberspace (Bush 2003). This program addresses the vulnerabilities of Supervisory Control and Data Acquisition (SCADA) systems a.k.a. Industrial Control Systems (ICS) and called for the public and private sectors to work together to foster trusted control systems. The SCADA/ICS systems are essential components for the effective operation of medium-to-large water and wastewater utilities in the U.S. The Homeland Security Presidential Directive (HSPD-7 2002) and its successor, the Presidential Policy Directive (PPD-21 2013), reaffirmed Water Sector as one of the 16 critical infrastructure sectors that must be protected.

Even with the establishment of formal critical infrastructure-related cyber security programs, since 2003 the threats have continued with increasing focus on critical infrastructure. In 2014, the Department of Homeland Security (DHS) responded to 245 incidents reported by asset owners and industry partners. Figure 7.1 is summary of the reported incidents. The data presented indicates that in 2014, the Water Sector reported the fourth largest number of incidents (tied with the communications sector) resulting in DHS incident response support behind Energy, Critical Manufacturing, and Healthcare (DHS 2015).

While U.S. Environmental Protection Agency (EPA) is the Sector-Specific Agency (SSA) lead for protecting the critical infrastructure in the Water Sector, it works collaboratively with the DHS, the utility owners, and operators, as well as representatives from industry associations to ensure that Water Sector cyber-protection and resilience strategies are effective and practical. The DHS serves as the cyber security lead SSA for the 16 critical infrastructure sectors and has cross-sector experience that is leveraged by EPA. This SSA lead-position was

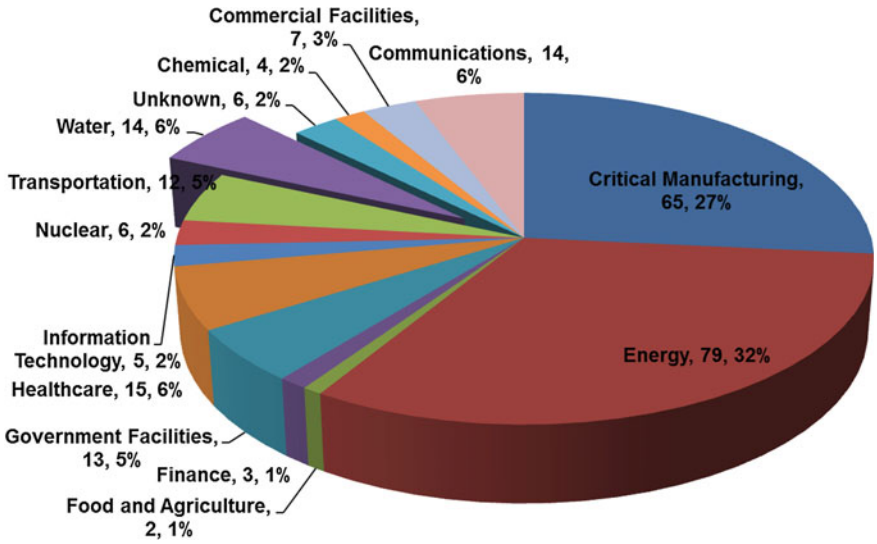


Fig. 7.1 The 2014 incidents report by sector (Reproduced DHS 2015)

clarified in response to section 10(a) of the Presidential Executive Order (EO) 13636 (Federal Register 2013) titled, "Improving Critical Infrastructure Cybersecurity," where the EPA reported that the Agency had the authority to establish cyber security requirements for the public water systems (PWSs) under the Safe Drinking Water Act (SDWA) section 1401; and the publicly owned treatment works (POTWs) i.e., the wastewater systems under the Clean Water Act (CWA) sections 304, 308, 402, and 501. Furthermore, for the purposes of cyber security, the EPA defines the Water Sector to include both water and wastewater utilities. However, there are some major differences in how the individual utilities operate because of differences in: size, population, finances, and regulatory focus.

The primary mission of a PWS is to focus on producing drinking water to meet their customer demand (e.g., firefighting, industrial, and residential needs) while simultaneously meeting the water quality requirements under the SDWA. Similarly, the POTWs are focused on treating the resulting wastewater both from municipal/industrial use and returning the treated water back to the environment; while meeting their regulatory obligations under the CWA. Due to the regulatory nature of the Water Sector, the culture is geared toward meeting regulatory compliance-driven goals. However, to manage cyber security risks, EPA as the Water Sector lead, has undertaken a collaborative voluntary partnership model. Specifically, under EO 13636 section 10(a) EPA has determined that current cyber security regulatory requirements in the Water Sector are sufficient. Therefore, a voluntary approach has been deemed adequate and the Agency is not proposing any regulatory actions under section 10(b). The section 10(b) of EO 13636 states that if

current regulatory requirements are deemed to be insufficient, agencies must propose prioritized, risk-based, efficient, and coordinated actions to mitigate cyber risk.

Organizationally, some PWSs and POTWs are combined, but a vast majority of them are separate entities. Numerically, there are many more PWSs than POTWs in the U.S. The sheer number of entities, and variations in size and staffing present their own sets of unique challenges. This chapter includes a profile of the Water Sector, an overview of the sector-specific cyber security framework, and provides information for the PWS and POTW managers that will help them create a cyber security culture within their organization. The information provided here is designed to assist PWS/POTW managers on how to deal with cyber risks and help them avoid common vulnerabilities. Sector-related case studies and data are also presented.

7.2 The Water Sector Profile

Water as a resource is more heavily used by other critical infrastructure sectors (e.g., electric and agriculture) than for water supply. The 2010 U.S. Geological Survey Circular 1405 (Maupin et al. 2014) estimates that the total water withdrawal in the United States is about 355 billion gallons per day (BGD) or 1.34 trillion liters per day (TLD). Similar to the previous 5-year estimates, thermoelectric power and agricultural irrigation continue to be the two largest users of water. The next largest user is the PWSs who withdrew 42.0 BGD or 0.16 TLD, or 11.8 % of the total. Circular 1405 also estimates that the number of people that received potable water from PWSs in 2010 was 268 million, or about 86 % of the U.S. population. Correspondingly, the EPA estimates that there are 155,000 PWSs that serve drinking water to more than 300 million people and 16,500 POTWs that serve more than 227 million people as well as certain industrial facilities (Grevatt 2014).

Withdrawal of water is where the Water Sector begins interaction with naturally available water resources. In the U.S., after water is withdrawn, it is treated to meet the requirements of the SDWA and its amendments prior to human consumption. The resulting wastewater is treated and discharged back into the natural environment for reuse. Water and wastewater utilities participation in this cyclical process is depicted as Fig. 7.2.

7.2.1 Public Water Systems (Drinking Water Systems)

EPA classifies PWSs based on the number of people they serve: (1) very small water systems serve 25–500 people, (2) small water systems serve 501–3300 people, (3) medium water systems serve 3301–10,000 people, (4) large water systems serve 10,001–100,000 people, and (5) very large water systems serve 100,001+ people. Figure 7.3 shows the estimated distribution of the PWSs in these

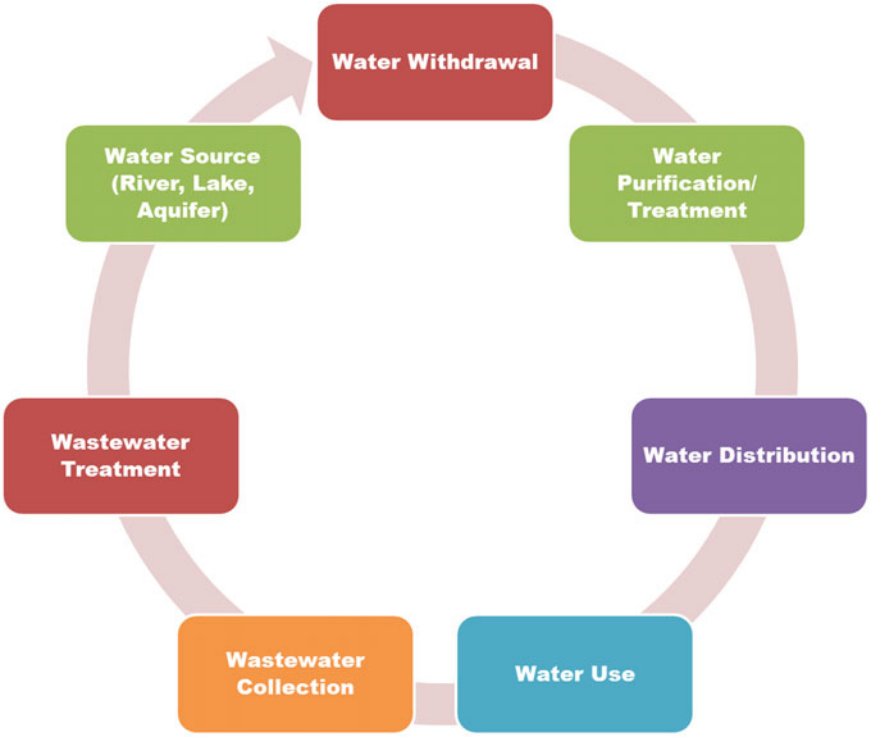


Fig. 7.2 The Water Sector water cycle

size categories and population served as reported by the EPA (2011; Panguluri et al. 2014).

Figure 7.3 shows that the majority of the drinking water systems are very small and small. This figure represents only the community water systems in the U.S. A community water system is defined by EPA to include PWSs that supply water to the same population year-round. Therefore these statistics exclude the transient/non-transient noncommunity water systems which, if included, would more than quadruple the number of very small systems (from 29,711 to 131,073) and bring the total closer to the 155,000 drinking water systems in the U.S. as reported by EPA. Overall, it is estimated that the cost of producing a thousand gallons of water (or 3785 L) in the U.S. can range between $3.37 for a very large privately owned PWS and $5.37 for a very small public PWS (Panguluri et al. 2014).

7.2.2 Public Owned Treatment Works (Wastewater Systems)

Wastewater is predominantly treated by POTWs, and EPA estimates of POTWs in the U.S. vary between 16,255 (EPA 2014) and 16,500 (Grevatt 2014, EPA-DHS

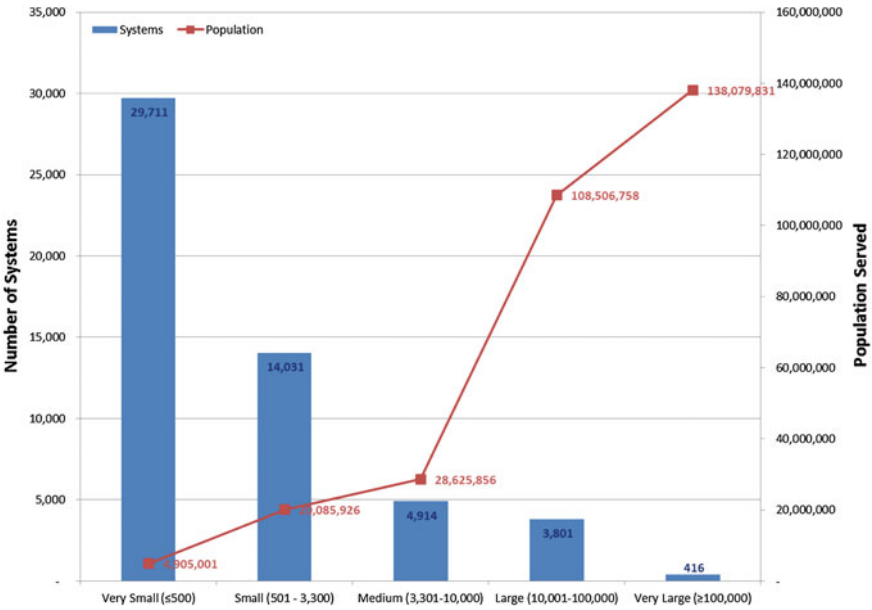


Fig. 7.3 Distribution of the PWSs by system size and population served

2010). EPA also estimates that 75 % of the total U.S. population is served by POTWs, and the remainder of the population is served by decentralized or private septic systems (EPA 2014). The distribution of POTWs by size and percentage of population served is shown in Fig. 7.4.

For the purposes of Fig. 7.4, POTWs that treat wastewater flows greater than 10 million gallons per day (MGD) or 37.85 million liters per day (MLD) are considered large; between 1 and 10 MGD (i.e., 3.785 and 37.85 MLD) are considered medium; and less than 1 MGD or 3.785 MLD are considered small. For purposes of determining the population served, 1 MGD or 3.785 MLD equals approximately 10,000 persons served (EPA 2014). Figure 7.3 was derived by combining population statistics from Safe Drinking Water Information System (EPA 2011) and the POTW size and flow data reported by EPA (2014).

This large variation in PWS/POTW system size and population served results in some economic and operational imbalances which can impact attitudes toward cyber security. The cyber security cultural approach presented in this chapter is designed to provide sufficient information for utility managers across the Water Sector.

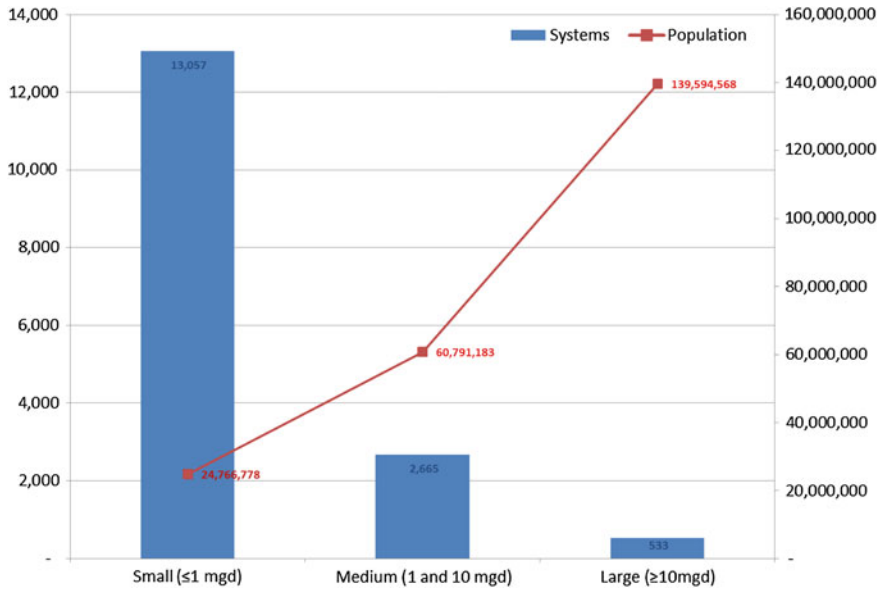


Fig. 7.4 Distribution of the POTWs by system size and population served

7.3 Cyber security Initiatives

The Water Sector has collaboratively partnered to plan and execute cyber security-related research and development activities. The sector-specific partners include: the EPA, DHS, the National Institute of Standards and Technology (NIST), the American Water Works Association (AWWA), the Water Research Foundation (WRF), the Water Environment Research Foundation (WERF), other water associations, educational institutions, national research laboratories, public and private research foundations, states/local agencies, PWSs, POTWs, and related organizations. Some of the collaborative cyber initiatives are highlighted in this section.

7.3.1 National Institute of Standards and Technology

NIST recently issued a document titled, "Framework for Improving Critical Infrastructure Cybersecurity" (NIST 2014). The cyber security framework presented in this document was developed by NIST in collaboration with other federal agencies and the private sector to provide guidance to organizations on managing cyber security risk. The "Framework" is a risk-based approach to managing cyber security and is composed of three parts: (1) the Framework Core, (2) the Framework Implementation Tiers, and (3) the Framework Profiles. Each

Framework component reinforces the connection between business drivers and cyber security activities (NIST 2014). A brief overview of these components is presented below.

7.3.1.1 Cyber security Framework Core

The "core" consists of five concurrent and continuous functions (Identify, Protect, Detect, Respond, and Recover) which, considered together, provide a high-level, strategic view of the lifecycle of an organization's management of cyber security risk. The core then identifies underlying key categories and subcategories for each function, and matches them with informative references such as existing standards, guidelines, and practices.

7.3.1.2 Framework Implementation Tiers

The "tiers" provide a context on how an organization views cyber security risk and the organizational processes in place to manage that risk. Tiers describe the degree to which an organization's cyber security risk management practices exhibit the characteristics defined in the framework (e.g., risk and threat aware, repeatable, and adaptive). The tiers characterize an organization's practices over a range, from Partial (Tier 1) to Adaptive (Tier 4).

7.3.1.3 Framework Profile

The "profile" represents the outcomes based on business needs that an organization selects from the framework of core categories and subcategories. The profile can be characterized as the alignment of standards, guidelines, and practices to the framework core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cyber security posture. Profiles can also be used to conduct self-assessments and communicate within an organization or between organizations.

A key objective of the NIST framework is to encourage organizations to make cyber security risk a priority, similar to financial, safety, and operational risk. The Framework relies on existing standards, guidance, and best practices. It provides a common method for organizations to assess their cyber security posture, describe a cyber security target state, prioritize opportunities for improvement, assess progress toward the target state, and foster communications among stakeholders (Stoner 2014).

7.3.2 Department of Homeland Security

The DHS has established the Critical-Infrastructure Cyber Community (C3) Voluntary Program as a partnership to increase awareness and use of the NIST Cybersecurity Framework. The C3 Voluntary Program is designed to connect Water Sector participants with DHS and other federal government programs to provide resources that will assist their efforts in managing their cyber risks. The C3 participants will be able to share lessons learned, get assistance, and learn about free tools and resources that can help them.

The DHS's United States Computer Emergency Readiness Team (US-CERT) leads efforts to improve the nation's cyber security posture, coordinate cyber information sharing, and proactively manage cyber risks to the Nation while protecting the constitutional rights of Americans. The US-CERT issues a weekly Cyber Security Bulletin that provides a summary of new vulnerabilities that have been recorded by the NIST National Vulnerability Database (NVD) in the past week. The NVD is sponsored by DHS's National Cybersecurity and Communications Integration Center (NCCIC) and the US-CERT.

US-CERT's sister organization, Industrial Control System Cyber Emergency Response Team (ICS-CERT), is the lead agency for assisting critical infrastructure, including water and wastewater, in securing their ICS/SCADA. ICS-CERT proactively helps utilities, vendors, and other critical infrastructure stake holders through online and class room cyber security training, on-site cyber assessments, vulnerability sharing, software tools such as the Cyber Security Evaluation Tool (CSET) and a web site that provides information on numerous topics for securing ICSs. ICS-CERT also assists operators of PWSs and POTWs that have been compromised by a cyber-attack with incident response services including forensics, malware, and digital media analysis conducted by subject matter experts in ICS-CERT's Advanced Analytical Laboratory (AAL). These services are free and can be used by the POTWs and PWSs to improve the cyber security posture of their ICSs.[1]

7.3.3 American Water Works Association

In an effort to provide PWSs with more actionable information on cyber security, AWWA has released the Process Control System Security Guidance for the Water Sector (AWWA 2014) and a supporting Use-Case Tool. The goal of the AWWA guidance is to provide water sector utility owners/operators with a consistent and repeatable recommended course of action to reduce vulnerabilities to cyber-attacks as recommended in the American National Standards Institute (ANSI)/AWWA G430 and the EO 13636.

[1] https://ics-cert.us-cert.gov/About-Industrial-Control-Systems-Cyber-Emergency-Response-Team.

The ANSI/AWWA G430 (Security Practices for Operations and Management) standard defines the minimum requirements for a protective security program for the Water Sector. It is designed to promote the protection of employee safety, public health, public safety, and public confidence. This standard is one of several in AWWA Utility Management series designed to cover the principal activities of a typical PWS or POTW. This AWWA standard has received the SAFETY Act designation from the DHS in February 2012.

The G430 standard is intended for all PWSs and POTWs regardless of size, location, ownership, or regulatory status. This standard builds on the long-standing Water Sector practice of utilizing a "multiple barrier approach" for the protection of public health and safety. The requirements of this standard are designed to support a protective utility-specific security program and are expected to result in consistent and measurable outcome. They address the full spectrum of risk management from organizational commitment, physical and cyber security, and emergency preparedness.

7.3.4 Environmental Protection Agency

As the Water Sector lead agency, the EPA encourages PWSs and POTWs to use the NIST Cybersecurity Framework and participate in the DHS Voluntary C3 Program. EPA continues to partner with the DHS, as well as the Water Sector Coordinating Council and Water Government Coordinating Council, to support the NIST Framework implementation. EPA promotes training of the PWS and POTW personnel on potential threats, vulnerabilities, and consequences from cyber threats, coupled with approaches to adopting and benefiting from the NIST cyber security framework. The voluntary cyber security framework provides a flexible performance-based and cost-effective approach to help PWSs and POTWs assess and manage cyber risk. The selected approach must also include provisions to protect business confidentiality, individual privacy, and civil liberties (Stoner 2014).

7.4 Cyber Security Risk

Water and wastewater managers and their Board of Directors have many things to worry about when it comes to managing a water system. Earthquakes, hurricanes, droughts, floods, supply shortages, interest rate increases, water supply, staffing shortages, regulatory changes, equipment failures, and union demands are just a few of the many events that negatively impact utilities' ability to deliver quality drinking water or treat sewerage. One of the main functions of management is to anticipate and mitigate potential problems. The differences in size and geographic location of an individual PWS and POTW result in each utility facing a unique set

of challenges. For instance, PWSs in California must prepare for droughts and earthquakes while PWSs situated along the Gulf coast are more concerned with floods and hurricanes.

Unfortunately cyber-attack is one risk that all utilities share unless they are a very small utility that does not use computers to monitor and control its processes or manage its business. However, even these organizations are not immune from the impacts of a successful cyber-attack against a supporting service provider like the electric utility. Given that cyber-attacks against the water sector are a growing problem, managers must learn to manage cyber risk just like they manage other risks. Before managers can effectively deal with the cyber risk they need to understand the various elements of cyber risk.

7.4.1 The Risk Equation

Cyber risk is often defined in terms of the risk equation which is

$$\text{Cyber Risk}(\text{R}) = \text{Threat}\,(\text{T})\,\text{X}\,\text{Vulnerability}\,(\text{V})\,\text{X}\,\text{Consequence}\,(\text{C}) \qquad (7.1)$$

Threat is the person who has the skills, capability, motivation, and access to compromise a computer system. A threat actor uses a variety of tools and techniques for attacking a system. These tools will be discussed later.

Vulnerability is the weaknesses in a control system and staff that an attacker can exploit to damage a control system.

Consequence is the impact caused by an attack (e.g., broken main, chemical overdosing, etc.).

Based on the risk equation, theoretically, a utility can eliminate its cyber risk by driving any one of the components in Eq. 7.1 to zero. Unfortunately, this is not practical, but steps can be taken to reduce the threat, mitigate vulnerabilities, and minimize the consequences of a successful attack thereby lowering the cyber risk. While the consequences of a successful cyber-attack will vary widely depending upon the individual incident type, location, utility size, staff and population served, the threat methodology, tools and vulnerabilities are common throughout the sector which are discussed in the following sections.

7.4.2 Advanced Persistent Threats

In an increasingly connected world, threats can originate from anywhere and be executed by anyone, but the advanced persistent threats (APTs) are usually the most dangerous. They are typically organized groups such as rival nation-states or terrorists that are highly committed and have vast resources to harm critical infrastructure targets.

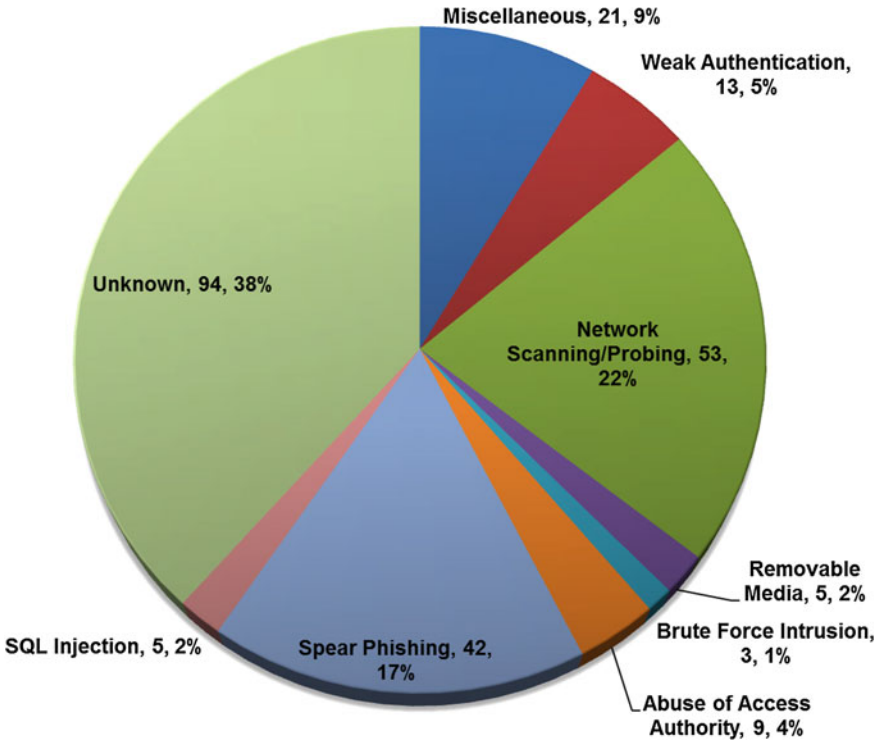


Fig. 7.5 Threat vectors of incidents (Reproduced DHS 2015)

Of the total number of incidents reported to ICS-CERT in 2014, roughly 55 % involved APTs or sophisticated actors. Other actor types included hacktivists, insider threats, and criminals. Figure 7.5 summarizes the reported incidents by type identified, the techniques used to gain access and manipulate these systems.

The APTs threat actors pick specific targets and goals, depending upon their objectives. Their objectives may include exfiltrating data, sabotage, and/or shutting down the process. In order to conduct any one of the goals, the APTs need to know the following specific information to accomplish their goals:

- Detailed design information of the control system and/or the process
- Access to the facility (electronically and/or physically)
- Understanding of the system(s) and process, and
- Knowledge of weaknesses and vulnerabilities that can be exploited to gain the required access

The process APTs follow to execute their goals is called the Kill Chain, which consists of the following activities:

- Reconnaissance—Prior to any cyber-attack, the APT threat actors will conduct reconnaissance and information gathering campaigns to acquire detailed

information in order to identify threat vectors and develop exploitation to gain access and carry out their intent. The threat actors will typically start out with Open-source intelligence (OSINT) to increase/decrease the level of severity of vulnerabilities. If a threat can find the entire system architecture, current software revision, accounts, passwords, defenses, and other information needed to achieve a threat goal, the vulnerabilities will all become high. To achieve significant damage/destruction and collateral damages (e.g., no water and panic from long-term utility outages), threats require detailed information about the system/sites on how to affect the SCADA/ICS system/site to operate in an unintended manner.

- Vulnerability—identification will then begin by developing a replica system to test against to find weakness and vulnerabilities that can be exploited. Then specific attacks and exploitations will be developed.
- Weaponization—the exploits will then be weaponized for delivery to gain access.
- Delivery—the exploitation package will then be delivered to the target by many different techniques in order to execute the exploit code.
- Exploitation—once the exploit code is executed, the aggressor will then have access to the network and systems where they will further conduct reconnaissance and gather additional information.
- Command and Control—The aggressors will then inject themselves within the system to have command and control capabilities through man-in-the-middle attacks or direct command execution.
- Execution—The aggressor will then execute their attacks to achieve their goals.

The following section will discuss hacking tools and techniques that APTs typically utilize to meet their objectives.

7.4.2.1 Hacking Tools

The APTs are commonly known to employ a variety of tools for hacking. Some of these hacking tools can also be used by the Water Sector utility technical managers to check for system vulnerabilities (with caution).

7.4.2.2 Phishing

Phishing (alteration of the term fishing) is the attempt to acquire sensitive information such as usernames, passwords, organizational information, and personal information by masquerading as a trustworthy entity in an electronic communication (Ramzan 2010). Phishing is typically carried out by email spoofing or instant messaging. These emails/messages generally contain links to websites that are infected with malware which often redirect users to enter sensitive information at a fake website whose look and feel are almost identical to a legitimate site that the

user often uses. Phishing is an example of a social engineering technique that is used to deceive users by and exploiting the poor usability of current web security technologies.

7.4.2.3 Fuzzing

Fuzzing is well established as an excellent technique for locating vulnerabilities in software. The basic premise is to deliver intentionally malformed input to target software and detect failure. A complete fuzzer has three components. A poet creates the malformed inputs or test cases. A courier delivers test cases to the target software. Finally, an oracle detects if a failure has occurred in the target. Fuzzing is a crucial tool in software vulnerability management, both for organizations that build software as well as organizations that use software (Knudsen 2015).

Fuzzers are an automated way of finding vulnerabilities by feeding the target application with a wide range of invalid input. Input which causes the application to respond abnormally or crash is then used to identify vulnerabilities. The fuzzer can look for specific kinds of vulnerabilities and can range from manual mode to fully automated. Vulnerabilities typically identified are application level overflows and format string vulnerabilities. They are best suited for services using documented protocols, standard servers, web applications, and protocols with many field-combinations (Phenoelit undated).

7.4.2.4 Nmap

Nmap ("Network Mapper") is an open source multi-purpose network scanning tool used mainly as an Internet Protocol (IP) port-mapper for network discovery and security auditing. The software is designed to identify open ports on each machine on the network. This information is used to identify the services that are running on each port. This is one part of the information gathering phase of a vulnerability assessment. The list of open ports on each machine gives a place to start testing for open holes into the SCADA system, but further analysis is required to not only verify the Nmap results, but also to query "unknown" ports returned by Nmap. Care should be taken when running this tool on a production machine when performing security tests because it can cause aberrant behavior. Nmap scans should be generally performed on a test or backup system if available (Lyon 2011).

7.4.2.5 Nessus

Nessus is an open-source remote security scanner that performs probabilistic analysis against a target system, detecting vulnerable services running on the scanned hosts and providing a warning level and recommended fix for each possible vulnerability (Riha et al. 2002). The Nessus output can be used as a starting

point for exploiting or testing a system. The Nessus output/report identifies possible vulnerabilities that the test team then tries to exploit, therefore verifying or disproving the SCADA system's susceptibility to that particular threat. It is not enough to report all vulnerabilities discovered in a Nessus scan as many of them may not actually affect the system and/or are false positives reported by Nessus. Conversely, Nessus may not detect all vulnerabilities and therefore, is only a starting point for assessing the system. Also, Nessus does not check for vulnerable installed software that runs locally on a computer (e.g., vulnerable versions of Internet Explorer).

7.4.2.6 Rootkits

A rootkit is a type of malicious software that is activated each time an infected system boots up. Rootkits are difficult to detect because they are activated and loaded to the system memory before the Operating System (OS) loads. Thus, a rootkit allows for the installation of hidden files, processes, hidden user accounts, and more in the infected system's OS. Rootkits can be designed to intercept data from terminals, network connections, and the keyboard (Beal 2015).

7.4.2.7 Backdoors

A backdoor in an electronic system is a method of bypassing normal authentication to secure access while remaining undetected. The backdoor may take the form of a hidden part of a program or a separate program (e.g., Back Orifice) which may subvert the system through a rootkit.

7.4.2.8 Social Engineering

In the context of cyber security, this refers to the psychological manipulation of people into performing unauthorized actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.

7.4.2.9 Hacking Techniques

In addition to the aforementioned tools for hacking, the APTs are commonly known to employ the following hacking techniques:

Sniffing

A sniffer is a program or device that can monitor (or sniff) data traveling in a network. Sniffers can be used both for legitimate network management functions and for stealing information from a network. Unauthorized sniffers can be extremely dangerous to a network's security because they are difficult to detect making it one of the favorite weapons in a hackers arsenal.

Decryption

Decryption is the process of converting encrypted data back into its original form, so it can be understood. Encryption and decryption should not be confused with encoding and decoding, in which data is converted from one form to another but is not deliberately altered so as to conceal its content.

Cross-Domain

A cross-domain technique is utilized to manually or automatically access or transfer information between two or more differing security domains or networks. These are integrated systems including hardware and software that enable transfer of information across domains.

Reverse Engineering

Reverse engineering is the process of extracting design information for electronic exploitation. The process often involves disassembling an electronic component or computer program and analyzing its contents. From a cyber security perspective, this task is generally performed with the intent of circumventing electronic access restrictions.

Sequential Query Language Injection

Sequential Query Language (SQL) is a programming language designed for managing data in a relational database management system (e.g., Oracle, SQL Server, etc.). SQL injection is a code injection technique, used to attack database applications. Many ICS systems contain a back-end database system to store data. In an SQL injection attack, malicious SQL statements are inserted into an entry field for execution (e.g., to dump the database contents to the attacker). The SQL injection technique is commonly used to exploit security vulnerabilities in an application's software. For example, an attacker can embed escape characters in SQL statements sent to a vulnerable database application that can result in

unexpected command execution. The embedded escape characters change the meaning of the characters which follow it, resulting in the execution of commands. SQL injection is more commonly employed as an attack vector on websites with back-end databases, but the technique can be used to attack other types of SQL databases.

Man-in-the-Middle Attack

A man-in-the-middle (MITM or MIM) attack occurs when the attacker secretly eavesdrops, relays, and/or alters the electronic communication between two parties. To successfully execute this attack, the attacker must be able to intercept messages passing between the two parties (or victims) and alter the content or inject new content. For example, if an attacker is within reception range of an unencrypted Wi-Fi wireless access point, he or she can electronically insert himself as a MITM, establish independent connections with the victims and relay messages between them. A successful MITM attacker makes the victims believe they are talking directly to each other over a private connection when, in fact, the entire conversation is controlled by the attacker.

7.5 Common Vulnerabilities

Historically, business and SCADA networks were separate because the network topologies were vastly different. Even if a utility owner recognized the value of integrating SCADA data into their strategic decision support systems, they could not because of limitation in the network topologies. The older SCADA systems relied heavily on serial connectivity and very low frequency radio communications that could provide enhanced range and partial line-of-sight connectivity, none of which supported standard IP connectivity desired by business networks (Panguluri et al. 2011). This virtual isolation also led to a false sense of security by many SCADA system administrators because they believed that because these systems were unconnected to the Internet, they could not be "hacked" into. Increasingly, the SCADA and business networks of most medium- to large-scale PWSs and POTWs are inter-connected to provide more integrated operation. However, if such integration were not secured properly, it will generally lead to greater vulnerability. The Water Sector is generally believed to lag most other critical infrastructures in securing their control systems (Baker et al. 2010; Weiss 2014). The following vulnerability categories continue to be identified as common issues the water sector faces. The top five areas of common security gaps are: (1) network configurations, (2) media protection, (3) remote access, (4) documented policies and procedures, and (5) trained staff.

1. Network configuration is one of the most critical elements of establishing a secured infrastructure to protect from cyber-attacks, yet one of the weakest links identified with critical infrastructure sites. Common issues include:
    a. Complete flat networks with no sub-netting or isolation of SCADA/ICS environments and business networks with direct connections to the Internet. These environments provide no security and are extremely vulnerable to cyber-attacks and electronic warfare.
    b. Interconnectivity between IT and SCADA/ICS zones through dual homed networks connected through a server farm or single historian database with dual network interface cards (NICs) installed that bridge a secured network to an unsecured network.
    c. Remote access and remote desktop connections made from unsecured and untrusted networks directly into the ICS environment, bypassing boundary protections and security.
    d. Direct connections from untrusted network systems (corporate systems and devices) directly to internal ICS network (i.e., no de-militarized zone [DMZ] implementations).
    e. Poor perimeter defenses with no zoning or network segmentation.
2. Media protections or portable media; such as universal serial bus (USB) keys, flash memory, compact disks/digital video disks (CDs/DVDs); are a crucial part of daily business. However, portable media is continually misused and easily lost or stolen which could cause a security breach. Improper use of media has been identified as a common issue where employees use unauthorized media within a control system, use media that is allowed on the corporate and ICS system without scanning, and use of personal media devices with the ICS system. Because portable media can also be lost, stolen, or compromised, it is essential to take precautions when using portable media devices. Portable devices should not be used in control systems environments that have been used outside of the control systems network. Devices should have encryption capabilities and should be "scanned" prior to use in sensitive or secure environments.
3. Remote access is another common finding where virtual private networks (VPNs) are allowed into the ICS/SCADA network for vendor support and after hour's operations. Many times companies use good security measures for remote access, but fail to verify and validate the security and integrity of the origination systems, which could already be compromised allowing a threat actor to piggyback on an authorized connection and gain access. Direct Internet connections to the ICS that bypass the security appliances need to be removed.
4. Policies and procedures are a core weakness. There are sometimes no policies or procedures to govern security. It is just an undocumented process, and the knowledge to perform good security is within each user/employee's domain. Without formally documented policies and procedures, a proper security culture cannot be established. The minimum policies and procedures that should be developed include:

a. Cyber security Plan
b. Access Control
c. Continuity of Operation
d. Configuration Management
e. Incident Response Plan
f. Backup and Recovery
g. Physical Security

5. Staffing\training—People are the foundational element for enforcing, managing, monitoring, tuning, responding to, and continually adapting and validating cyber security controls and practices employed throughout ICS systems. The core issue is generally the available staffing levels are insufficient to maintain current operations and implement cyber security recommendations. Due to staffing issues, the employees only have time for operations and putting out "fires," and never have time to learn, design, and implement security technologies, techniques, and capabilities to defend their networks.

7.5.1 Consequences

Once a threat actor has identified system vulnerabilities, he or she will use the tools and techniques outlined in the Hacking tools section to launch an attack. The attack will generate cyber-impacts that will affect the confidentiality, integrity, or availability of the data/system. In other words, the attacker will either try to steal documents or data, change files or data, and/or deny the use of the system.

The cyber-impacts in turn may have process impacts. These impacts will vary depending on the process and how the water/wastewater system is designed. For instance in a PWS, if an attacker changes database parameters in the real-time database (impacts system integrity) they could turn on pumps causing a distribution tank to overflow. The individual process impacts can be catastrophic or relatively benign depending on how the tank's overflow structure is designed. If the tank safely funnels the water to a nearby stream (provided chlorinated water is not an issue) the impacts are relatively minor. However, if the overflow water washes out the hillside, it could undermine the tank's foundation and/or damage houses and structures below the hill. Alternatively, there may be no process impacts. For example, if non-cyber devices (such as an altitude valve or high-pressure switch) on the pump's discharge line can override the control system by turning the pumps off, when it locally detects that the tank level is too high.

Similarly, the POTWs are also susceptible to the impacts of a cyber-attack. For example, a denial-of-service (DoS) attack (which impacts system availability) on a control system that is responsible for sewerage digestion could potentially kill the microorganisms responsible for breaking down the organic material.

Ultimately, the process impacts on a water and wastewater system could result in life, safety and health issues, equipment/capital losses, and environmental damage

to both the utility and the customers they serve. The overall economic, societal/environmental, and psychological consequences of a successful attack will vary widely depending upon the equipment, location, and resulting damage. Quantifying the various costs of individual attacks is a difficult task. While the consequence may be minimal from a specific aspect, they may be devastating in other aspects. An often cited example of a successful water sector attack is the attack on the Maroochy Shire POTW in Queensland, Australia (Panguluri et al. 2004; Weiss 2014). The attack resulted in raw sewage spill into rivers, parks and the grounds of a nearby hotel. The main consequence in this case, was environmental damage and societal costs.

The attack was conducted by a former insider Vitek Boden. Mr. Boden formerly worked for Hunter Watertech, an Australian firm that originally installed the SCADA radio-controlled sewage equipment for the Maroochy Shire Council. Between February 28, 2000 and April 23, 2000, Mr. Boden issued radio commands to the sewage equipment on 46 separate occasions that resulted in spills. During this period, the sewerage system experienced the following series of faults (Weiss 2014):

- Pumps were not running when they should have been,
- Alarms were not reporting to the central computer,
- A loss of communication occurred between the central computer and various pumping stations.

Another employee of Hunter Watertech was appointed to review the aforementioned series of faults. He began monitoring and recording all signals, messages, and traffic on the radio network. As a result of his investigations, he (along with other experts) concluded that many of the problems were the result of human intervention rather than equipment failure. Additionally, the faults associated with the attack ceased after Mr. Boden was arrested.

7.5.2 Creating Cyber Security Culture

Unfortunately because of the variety of threats, vulnerabilities, and consequences there is no single solution to reduce cyber risk. In fact, the best strategies for securing ICS/SCADA are dependent on a multi-layered approach called defense in depth. This approach applies many defensive strategies designed to prevent, deter, and/or slow the progression of an attack. Making it as difficult as possible for an attacker to reach their objective not only increases their exposure to discovery, but it gives the utility time to detect and respond to the attack.

Because most water managers are unfamiliar with IT and ICS/SCADA technology, much less cyber security defenses, they understandably turn to their technical staff to protect their systems. This leads to a bewildering world of encryption, DMZs, segmenting, firewalls, intrusion detection systems (IDS),

patching, auditing, logging, anti-virus software, etc. While these technical measures are crucial for developing a strong defense in depth program they are only one leg of a three-legged stool. The other two legs are equally important. They are: people and processes. If you remove any one of these legs and, like a stool, the cyber defenses are less stable and more vulnerable to tipping over.

While it is understandable why a manager would transfer the responsibility for the cyber defenses of the utility's ICS/SCADA to the technical staff, this approach often erodes or neglects the other two legs of the stool; people and processes. Like managing any risk, a utility manager, the board of directors, or city government, must take ownership of ICS/SCADA cyber security. They may not have the technical expertise for bolstering the cyber defenses of their control systems, but they do have the responsibility for selecting and managing people and ensuring that the proper processes are developed and followed.

Selecting the right people with the skill set to secure a control system is a challenge. Just to maintain a control system requires knowledgeable individuals who are familiar with the process, instrumentation, programming and configuring embedded devices (programmable logic controllers (PLC), remote terminal units (RTUs), routers, etc.), local area networks, wide area networks (WANs), operating systems, databases, radios, ICS applications, and so on. Securing these systems requires additional skills, plus an awareness of existing and emerging threats and exploits.

In larger PWSs and POTWs, the ICS or SCADA group typically resides in the operations & maintenance (O&M) department although it is also common to see the IT department support the control system. Each approach has advantages and disadvantages. When under the O&M umbrella, the SCADA/ICS group typically responds faster to operational issues. It is also easier to coordinate ICS outages and projects. When under the IT umbrella, the control systems are usually better secured and integrated with the enterprise network. A few utilities have successfully adopted a hybrid-model where an IT person has been assigned to the SCADA group to help the control system engineers secure and maintain their system.

Irrespective of the organizational model used to maintain the ICS, the managers need to ensure that the IT/SCADA/ICS staff are knowledgeable and trained on cyber security. This can be accomplished through strategic hiring, training, and/or mentoring by internal IT staff or external consultants/vendors. The hybrid-model suggested above is an ideal mechanism for mentoring and training.

Training should also be given to all stakeholders who interface with the control system, not just the SCADA staff. Operators, maintenance technicians, engineers, and other staff who use the system should understand their roles and responsibilities.

Users and administrators roles and responsibilities should be documented in policies and procedures. The processes established by the policies and procedures should cover everything needed to securely and reliability maintain the control system as well as the "dos" and "don'ts" when interfacing with the system. This includes backups, account management, acceptable use, auditing, portable media policy, change management, system monitoring, etc. While most SCADA

engineers are good at what they do, the demands on their time leave little time for writing policy and procedures. Most of the "tribal knowledge" for maintaining the system is poorly documented or not documented at all. Here again it is the managers' job to ensure that the proper processes, based on policy procedures, are implemented and followed. Managers can help by providing the resources needed to develop policy, procedures, and processes.

In short, it is the manager's responsibility to cultivate a cyber security culture in their utility. Without a strong cyber security culture, there is no cyber security. Although some companies have established a cyber security culture within their organizations, most companies have made little progress. They tend to be reactive rather than proactive. When budgets get tight, security programs and departments are the first to be cut (Fisher 2014).

To shift from a reactive to a proactive organization, a manager must take the lead by changing the culture in the organization. Fisher lists an eight-stage process for creating major change (Fisher 2014):

- Establishing a sense of urgency—Identify and discuss the crises or potential crises
- Creating the guiding coalition—Putting together the group with the power to lead change
- Developing a vision and strategy
- Communicating the change vision
- Empowering broad-based action
- Generating short-term wins
- Consolidating gains and producing more change
- Anchoring new approaches in the emergent culture

Applying these principles to change the culture of the organization will help ICS stake holders understand their responsibilities for protecting their ICS. Establishing a cyber security culture is the framework for implementing a strong defense in depth program. It puts the three legs (technology, people, and processes) of cyber security on a firm foundation.

7.6 Secured Network Design

A review of historical data from PWSs and POTWs reveals a wide variety of cyber security practices. Over the years, many have improved their security posture from minimal or no cyber security posture, to poster child examples of the best security posture observed. Generally, the best cyber security designs strive to limit access or incorporate isolation capabilities of ICS/SCADA systems. The isolation of ICS system can be achieved by establishing security enclaves (or zones) with virtual local area networks (VLANs) or subnets that are segregated from lower security

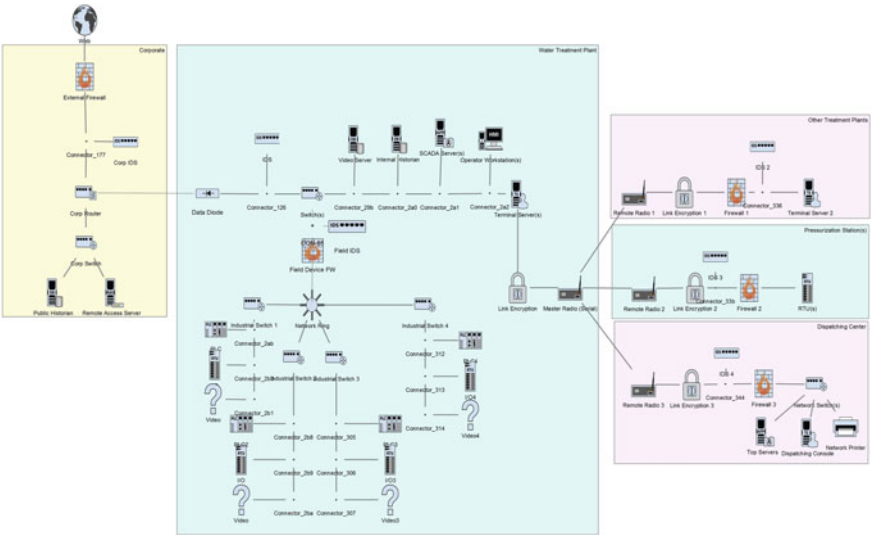


Fig. 7.6 Secure PWS architecture example

zones like corporate networks or any Internet accessible zones. Figure 7.6 illustrates an example of a secure PWS architecture.

In this example design, the architect has isolated the ICS environment with no ingress electronic connections. The use of data diodes between the SCADA/ICS and corporate IT environments allows for information sharing from the ICS environment through a truly one-way transfer of data from ICS historians (databases) for business needs and reporting. The use of true isolation through data-diode technologies between the treatment plant ICS and corporate environment (as shown in secure PWS Architecture example—Fig. 7.6) is more recent. The adoption of this technology within the water sector has been observed at one utility. The use of data-diode technology is now gaining increasing acceptance within the Water Sector. Some PWSs have identified the use of this technology in their advance security posture planning documents. The implementation of this technology requires at least two full-time-equivalent (FTE) technology staff resources for several months during the development, testing, verification and deployment phases. Additionally, depending upon the complexity of the architecture, a successful deployment may require three or more FTEs. After the full implementation and optimization of the secure PWS architecture, it is estimated that at least 1/4 to 1/2 FTE ongoing resources will be necessary to manage and support this type of security posture. Based on current water sector cyber security implementation and execution costs, it is estimated that this type of technology implementation (depending on the features) would average around $300,000 for initial implementation and optimization.

The application of secure architecture and isolation of the ICS environment prevents remote access connection and prevents unauthorized computers or

network devices including 3rd party vendors from entering into the ICS environment. Prior to adding a network device or computer to the ICS environment, a thorough analysis is conducted, and then the equipment is reviewed and approved for use. Once approved, the equipment stays at a secure off-site location for future use and is identified as an ICS component.

Based on this design, the threat vectors are dramatically reduced to insider threats and media protection for required updates, modifications, and enhancements to the environment. Additionally to the ICS environment, the ICS cyber security team should enable port security with Media Access Card (MAC) filtering to eliminate the capabilities of a threat actor who can gain physical presence for unplugging approved components and attempt to use the connection to gain electronic access to the system. All unused ports are disabled, and if an attempt is made to take over a connection, they system will identify a rouge device on the network and shut off the port and report to the cyber security team.

Further mitigations should also be incorporated for secure management of each component (e.g., with software and OS restrictions by policy). The system administrators can develop a "gold-disk" standard for the OS, and allow a user to only install preapproved applications. This guarantees that specific systems, applications and patches are installed and up-to-date. Least privileges methodology should also be used (i.e., only grant the level of access needed to perform their job), and restrictions are in place for users to install or run specific applications, device link libraries (DLLs) for any removable media. This is accomplished by the use of an ICS active directory (AD) in Windows architecture that allows for central management of groups, policies, and user authentication. Application white-listing can also be enabled to only allow approved applications to run within the environment.

In a "secure architecture," the perimeter defenses should also be very verbose with restricted firewall rules for egress and ingress at each internal ICS zone. Only the required traffic between zones should be allowed and configured to specific IP addresses/ports with all other communications explicitly denied. In the event that the corporate environment becomes compromised, the ICS environment has the ability to isolate and avoid any possible infections, because of the data diode deployment. Internally, however, if the ICS environment is ever infected or compromised through media, then the capability should exist to isolate the field equipment, which will continue to run basic configuration or current logic of last known commands. The system should be designed to fail-safe and continue to operate as designed. At each perimeter per enclave, IDS should be deployed to monitor and alert to any abnormal behaviors, and to validate the rules sets on the firewalls are working as designed.

All ICS internal communications to other facilities or ICS process over a WAN connection should be fully encrypted through Internet Protocol Security (IPSEC) tunnels or link encryption, and all Web servers, telnet, and network discovery services should be disabled.

The suggested architecture along with strong policies and procedures is necessary in order to develop a security culture and to raise the level of awareness of each

employee with management support for training of the core cyber security staff for cyber security skills enhancements and development.

A security information and event management (SIEM) system should also deployed for central management of monitoring appliances for log reviews and alerting capabilities in the event that the system starts to identify anomalies with the systems for early detection, alerting and recovery capabilities.

These types of measures will result in a strong security design. Finally, when excessing or decommissioning equipment, proper equipment disposal process should be in place to ensure no proprietary information ever leaves the environment. A proper disposal process protects from malicious reverse engineering, discovery, and reconnaissance activities.

7.7 Summary and Conclusions

Based on the incidents reported and documented in this chapter, it is clear that the cyber threats to the water sector are real. The insider attack on the Maroochy Shire POTW provides an insight into the real consequences of a specific attack. It is imperative that the PWSs and POTWs adopt suitable countermeasures to prevent or minimize the consequences case of cyber-attacks. The greatest challenge for the water and wastewater industry is the large variance in size, staffing, and resources available to the individual utilities. Also, the utilities must rise to meet this challenge by voluntarily adopting countermeasures in phases that best meets their security and organizational requirements. A sector-specific secure design architecture example is provided in this chapter to guide the PWSs and POTWs to refine their approach to cyber security. The utilities must use the available resources to create a culture that prepares and implements programs that are designed to improve cyber security. Utilities should avail the free opportunities available through DHS to train their staff and allocate necessary funding to achieve improvements in cyber security.

References

AWWA. (2014). Process control system security guidance for the water sector. AWWA Government Affairs Office, 1300 Eye St. NW, Suite 701 W, Washington, DC 20005.

Baker, S., Waterman, S., & Ivanov, G. (2010). In the crossfire—Critical infrastructure in the age of cyber war. A global report on the threats facing key industries. McAfee International Ltd, 100 New Bridge Street, London EC4 V 6JA, UK.

Beal, V. (2015). Rootkit, webopedia. http://www.webopedia.com/TERM/R/rootkit.html

Bush, G. W. (2003, February). *National strategy to secure cyberspace*. Washington: The White House.

DHS. (2015). ICS-CERT year in review industrial control systems cyber emergency response team 2014. *Issued by DHS's national cybersecurity and communications integration center*. Accessed April 26, 2015 from https://ics-cert.us-cert.gov/Year-Review-2014

EPA. (2011, June). Fiscal year 2010 drinking water and ground water statistics. EPA office of ground water and drinking water. EPA 817K11001.

EPA. (2014). Basic information about water security. Accessed March 28, 2015 from http://water.epa.gov/infrastructure/watersecurity/basicinformation.cfm

EPA-DHS. (2010). Water sector-specific plan, an annex to the national infrastructure protection plan. Office of Ground Water and Drinking Water, Water Security Division, EPA 817-R-10-001.

Federal Register. (2013, February 19). *The presidential executive order 13636—Improving critical infrastructure cybersecurity* (Vol. 78 No. 33).

Fisher, R. (2014, October 16). *Applying culture change in cyber security to enhance homeland security*. Colorado Technical University Doctoral Symposium.

Grevatt, P. C. (2014, May). EPA response regarding executive order 13636, adoption of the cybersecurity framework by the water sector. A letter to the White House dated.

Homeland Security Presidential Directive 7 (HSPD-7). (2002). Directive on critical infrastructure identification, prioritization, and protection. Issued by the White House, December 17, 2003.

Knudsen. (2015). What is fuzzing: The poet, the courier, and the oracle. Article date January 7, 2015. Available at http://www.codenomicon.com/resources/white-paper/pdf/WhatisFuzzing.pdf

Lyon, G. (2011). The official Nmap project guide to network discovery and security scanning. Copyright Insecure.Com LLC, Book. http://nmap.org/book/ ISBN: 978-0-9799587-1-7

Maupin, M. A., Kenny, J. F., Hutson, S. S., Lovelace, J. K., Barber, N. L., & Linsey, K. S. (2014). Estimated use of water in the United States in 2010: U.S. Geological Survey Circular 1405, 56 p. Accessed March 28, 2015 http://dx.doi.org/10.3133/cir1405

NIST. (2014). Framework for improving critical infrastructure cybersecurity, Version 1.0, National Institute of Standards and Technology, February 12, 2014. Accessed March 28, 2015 from http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

Panguluri, S., Haji, S., Adams, J., & Patel, A. (2014). Drinking water purity—a market outlook. In S. Ahuja (Ed.), *Comprehensive water quality and purification* (Vol. 2, pp. 1–18). United States of America: Elsevier.

Panguluri S., Phillips, Jr. W. R., Clark R. M. (2004). Cyber threats and IT/SCADA System vulnerability. In: Mays L.W. (Ed.) *Water supply systems security* (5.1–5.18). McGraw-Hill, New York.

Panguluri, S., Phillips, W. R, Jr, & Ellis, P. (2011). Cyber security: Protecting water and wastewater infrastructure. In R. M. Clark, S. Hakim, & A. Ostfeld (Eds.), *Handbook of water and wastewater systems protection* (pp. 285–318). New York: Springer-Science.

Phenoelit. (undated). Bug hunting—Vulnerability finding methods in Windows 32 environments compared FX of Phenoelit. Accessed April 26, 2015 http://www.phenoelit.de/stuff/Bugs.pdf

Presidential Policy Directive-21 (PDD-21). (2013). PDD-21—Critical infrastructure security and resilience. Available at https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

Ramzan, Z. (2010). Phishing attacks and countermeasures. In P. Stavroulakis., & Stamp, M (Eds.) *Handbook of information and communication security* (443–448). Springer. ISBN 9783642041174.

Riha, D. S., Thacker, B. H., Enright, M. P., Huyse, L., Fitch, S. H. K. (2002). Recent advances of the nessus probabilistic analysis software for engineering applications. AIAA 2002-1268. http://www.nessus.swri.org/publication_files/2002_AIAA_1268.pdf

Stoner, N. (2014). Reducing cybersecurity risks in the water sector: A voluntary partnership approach. Blog dated February 12, 2014. Accessed March 28, 2015 http://blog.epa.gov/epaconnect/2014/02/reducing-cybersecurity-risks-in-the-water-sector-a-voluntary-partnership-approach/

Weiss, J. (2014). Industrial control system (ICS) Cyber security for water and wastewater systems. In R. M. Clark., S. Hakim (Eds.), *Securing water and wastewater systems, protecting critical infrastructure* 2. Switzerland: Springer International Publishing. doi 10.1007/978-3-319-01092-2_3

Chapter 8
The Community Cyber Security Maturity Model

Natalie Sjelin and Gregory White

Abstract Cyber threats at the community level have become increasingly sophisticated and targeted and are occurring more frequently. Hackers and cyber criminals no longer need to be in the proximity of a target. An attacker can be anywhere in the world, which makes it almost impossible to locate and identify the source of an attack. Most government agencies, industry partners, critical infrastructures, school systems, nonprofit organizations, and other organizations exist and operate at the local level and are not equally prepared to defend against cyber threats that could affect the entire community. In 2002, the Center for Infrastructure Assurance and Security (CIAS) at The University of Texas at San Antonio (UTSA) conducted, Dark Screen, a community cyber security exercise in San Antonio, Texas. The exercises highlighted how services such as critical infrastructures and emergency services could be delayed and/or disrupted. They provided awareness as to how business and local governmental operations could be impacted by a cyber-attack and helped identify resources and capabilities to prevent, detect, and respond to a cyber security event. As a result of this effort, the CIAS created the Community Cyber Security Maturity Model (CCSMM) to provide guidance on how to respond to cyber threats at the community level. A program was developed to help communities (and states) implement the model. The CIAS initially worked with communities in seven states helping them begin development of their own programs. The specific areas a community needs to improve when it deals with cyber threats include awareness, information sharing, policies, and planning. One of the important features of the CCSMM is that it provides guidance as to how to improve a local community's ability to protect against cyber vulnerability.

N. Sjelin (✉) · G. White
Center for Infrastructure Assurance and Security,
University of Texas at San Antonio,
One UTSA Circle, San Antonio, TX 78249, USA
e-mail: Natalie.Sjelin@utsa.edu

G. White
e-mail: Greg.White@utsa.edu

R.M. Clark and S. Hakim (eds.), *Cyber-Physical Security*,
Protecting Critical Infrastructure 3, DOI 10.1007/978-3-319-32824-9_8

Acronyms

CCSMM	Community Cyber Security Maturity Model
CERT	City Computer Emergency Response Team
CIAS	Center for Infrastructure Assurance and Security
COOP	Continuity of Operations Plans
DHS	Department of Homeland Security
DoD	Department of Defense
DRP	Disaster Recovery Plans
EOP	Emergency Operation Plans
ISAC	Information Sharing and Analysis Center
ISSA	Information Systems Security Association
NCPC	National Cyber security Preparedness Consortium
NIST	National Institute of Standards and Technology
PPD-8	Presidential Policy Directive 8
SANS	Institute Escal Institute of Advanced Technologies
SOP	Standard Operating Procedures
USTA	The University of Texas at San Antonio

8.1 Introduction

On almost any day, it is possible to read about a new cyber security breach that is impacting the public. The cyber threat is becoming increasingly sophisticated and attacks are more targeted and are occurring more often than in the past. Even if we have done everything we can to protect our personal information, we are still vulnerable to a cyber incident whether directly targeted in the attack or as a victim of a larger data breach. Criminals today no longer need to be in the local proximity of an incident. An attacker can now be anywhere in the world, which makes it much harder to identify and locate who is behind the cyber-attack, cyber crime, or cyber event.

Attacks on communities have taken critical services offline for periods from hours to days. Clearly cyber security programs are needed in order for communities to become better prepared to face cyber threats. In 2002, the Center for Infrastructure Assurance and Security (CIAS) at The University of Texas at San Antonio (UTSA) conducted, Dark Screen, a community cyber security exercise in San Antonio, Texas. These exercises provided awareness as to how business operations could be impacted by a cyber-attack and helped identify resources and capabilities to prevent, detect, and respond to a cyber security event. The exercises highlighted how services such as critical infrastructures and emergency services could be delayed and/or disrupted.

As a result of the exercises, the CIAS created the Community Cyber Security Maturity Model (CCSMM) to provide guidance on how to respond to cyber threats at the community level.

After establishment of the model, the CIAS began developing a program to help communities (and states) implement the model. The CIAS initially worked with communities in seven states helping them begin development of their own programs. The CCSMM addresses specific areas a community needs to improve when it comes to cyber threats. The areas are awareness, information sharing, policies, and planning. One of the important features of the CCSMM is that it provides guidance as to how to improve a local community's ability to protect against cyber vulnerability. These issues will be addressed in-depth in the following discussion.

8.2 Improving the Cyber security Posture in Communities

Cyber threats are outpacing our ability to prepare for them. At the community level —where government agencies, industry partners, critical infrastructures, school systems, nonprofit organizations, and other organizations exist—we recognize that organizations are not prepared equally to defend against cyber threats that could affect the entire community. There have been attacks on communities that have taken services such as 911 offline for hours to several days. Some targeted attacks have taken other public services off line for extended periods of time causing communities to realize we simply are not prepared. From New York City, which suffered an attack in February 2015 that shut down government email systems to Napa Valley that was hit with a denial-of-service attack in 2014, cities across the nation are increasingly the targets of a variety of cyber-attacks (Enbysk 2015).

A cyber security program is needed for communities to become better prepared for the cyber threats they face. This is increasingly important because response to an event impacting a community will begin at the local level. The understanding of how and when to respond, and who to request assistance from including who ultimately will make cyber response decisions for the community, must be in place prior to an event occurring.

8.2.1 History of the CCSMM

In 2002, the CIAS at the UTSA conducted the first community cyber security exercise in San Antonio, Texas, called *Dark Screen*. This tabletop exercise proved extremely successful at helping community leaders become aware of how an attack on the cyber infrastructures in the community could impact the community at large (White and Sanchez 2003; Goles et al. 2005). After completion of this exercise, the CIAS began conducting a series of similar exercises for other communities. Funded by the Department of Defense, the CIAS concentrated on communities "in which

there is a significant DoD presence." All these subsequent exercises were also very successful in bringing to light the issue of cyber security and the need to be prepared to address cyber incidents when they occur. The goals of the Community Cyber Security exercises were to provide awareness to the various sectors within the community of how business operations could be impacted by a cyber-attack and to identify resources and capabilities to prevent, detect, and respond to a cyber security event. The exercises highlighted how services such as critical infrastructures and emergency services could be delayed and/or disrupted and show how interdependent the community is. A coordinated cyber-attack on a community could have devastating cascading effects impacting the whole community. One of the more dramatic examples of cascading effects in a critical infrastructure, though not caused by a cyber-attack, was the blackout of 2003 that impacted the Northeast and Midwest. In this incident, a problem in western New York and Canada resulted in a series of power failures in eight states in the Northeast and Midwest (Barron 2003). This, of course, impacted both government and industry in these states illustrating the impact to other sectors as well.

After several exercises were conducted, the CIAS took a step back to see how well the communities had addressed the issues raised during the events. What was discovered was that while the community leaders still knew cyber was something that they needed to be concerned with, after a year they had almost universally not done anything to improve their cyber security posture. They still understood that a cyber security program needed to be implemented and that public and private partnerships needed to be established. Additionally, they had discovered that there were a number of vendors who were willing to provide services and technology, but the communities did not know what to purchase nor did they know exactly how to begin building and implementing a community-wide program to address cyber threats. What was needed first? What should their first step be? What was lacking was any coordinated plan to help communities (and by extension, states) get started on developing a viable and sustainable cyber security program.

8.2.2 Purpose and Intent of the CCSMM

As a result of the analysis of effectiveness of the exercises and the issues that communities faced, the CIAS created the CCSMM to provide guidance on how to begin. The CCSMM provides three critical features

1. A *yardstick* which can be used to measure the current status of a community's cyber security program and posture,
2. A *roadmap* to help a community know what steps are needed to improve their security posture, and
3. A *common point of reference* that allows individuals from different communities and states to discuss their individual programs and relate them to each other.

After establishment of the model, the CIAS began development of a program to help communities (and states) implement the model. The CIAS initially worked with communities in seven states helping them begin development of their own programs.

The CCSMM is an involved model with many factors that need to be addressed in establishing a cyber security program in a state or community. It is organized into focus areas or dimensions and identifies five levels of improvement in the roadmap showing how to build a cyber security program in a community or state.

8.2.3 CCSMM Overview

The CCSMM was developed to provide states, communities, or local jurisdictions with a framework to identify what is needed to build a cyber security program that addresses "whole community" response at the local level for a cyber incident or attack. It is a guide allowing leaders to establish a baseline at the local level. The baseline can then be used to identify isolated cyber incidents that impact one organization or sector but can also be used to identify cyber incidents being used as a coordinated attack impacting cross-sector organizations and agencies in a specific geographic area.

Although many jurisdictions realize that cyber threats should be addressed, many struggle with what is needed to establish a local cyber security program that includes cross-sector identification and response for cyber incidents. The strategies identified in the CCSMM framework go beyond simply protecting systems and networks within local government agencies. They are designed to assist a community in identifying what needs to be done in building a viable and sustainable cyber security program. With a viable program, communities will be prepared to detect a cyber-attack, develop plans to respond during an attack, and determine what to do after an attack has occurred.

The model addresses specific areas that a community needs to improve when it comes to cyber threats. The areas of improvement are called *dimensions*. There are four dimensions identified in the CCSMM. They are **awareness**, **information sharing, policies,** and **planning**.

Each of these dimensions has five levels of maturity. The levels begin at the **Initial** level (Level 1), which is where every community begins, and builds a roadmap for communities to improve to reach a **Vanguard** level (Level 5). Level 5 is the stage where cyber security is a business imperative and is simply incorporated into every aspect of government, industry, and public life. The improvements are accomplished with *implementation mechanisms*. The implementation mechanisms allow us to progress from one level to the next in each dimension. The implementation mechanisms are the activities used to

- Increase awareness
- Establish information sharing practices

- Add cyber components to policies in a meaningful way
- Incorporate aspects of cyber security into continuity plans

The implementation mechanisms are

- Metrics
- Processes and procedures
- Technology
- Training
- Assessments

While the CCSMM was created and implemented in the 2006 timeframe, the importance of this and other frameworks designed and created to address the "whole community" to prepare for threats and hazards was recognized officially by the White House in 2011. The Federal Government recognized that a cross-sector, public and private approach would be necessary to prepare for the cyber threat and that preparedness is a shared responsibility. Presidential Policy Directive/PPD-8: National Preparedness was signed by the President on March 30, 2011 (PDD-8 2011). In the directive, the Secretary of Homeland Security was directed to coordinate a campaign that included community-based programs to enhance national resilience. The directive was "aimed at strengthening the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk to the security of the Nation, including acts of terrorism, cyber-attacks, pandemics, and catastrophic natural disasters." It is important to note that cyber-attacks were listed second on the list of threats that pose the greatest risk to the nation.

An important point made in PDD-8 is the need for community-based approaches to addressing the threats. To do this in the cyber arena where computers and networks are found in every sector as well as our private lives, a "whole-community" approach is required. The whole community is generally defined as the following:

- Individuals and families, including those with special access and functional needs
- Businesses
- Faith-based and community organizations
- Nonprofit groups
- Schools and academia
- Media outlets
- All levels of government, including territories and tribal nations.

8.3 CCSMM in Depth

In order to completely understand the individual components of the CCSMM and how they interact, knowledge of the areas in which we need to improve our cyber security posture is needed. There are four areas of improvement called *dimensions*.

The dimensions, as previously mentioned, are **awareness**, **information sharing**, **policies,** and **planning**. Communities may work on one or all of the dimensions at the same time. There may be one dimension that is easier to address in your community than others. While this discussion uses the term "community" in describing the model, all aspects of the model apply equally as well to states, territories, and tribal jurisdictions.

8.3.1 Dimensions

8.3.1.1 Awareness

The purpose of this dimension is to ensure members of the community understand the overall cyber threats they face. Most people understand that cyber threats exist, however, not as many understand the scope of this threat, the current attack trends, how a cyber incident can impact a community, what the vulnerabilities are that should be addressed, and what the cascading effects may be if a community was under a cyber-attack. As communities mature in their awareness they will need to address the following questions:

- What is the level of awareness about cyber security issues within the community?
- How is this awareness level maintained?

8.3.1.2 Information Sharing

The information sharing dimension addresses what cyber-related information organizations will share both internally and externally. If an organization is willing to share certain types of cyber-related information, who specifically will they share it with both inside and outside of their organization, and in what time frame should they share it? A related and equally important question is how will the information be shared. This, in particular, is one aspect of this dimension that will change significantly as the organization matures in their security processes. The dynamic of sharing information about cyber incidents or attacks is a difficult one. There is a hesitancy to share cyber-related information. With this in mind, how do organizations overcome these challenges? If everyone shared all information in regard to their cyber infrastructures, would this generate an information overload situation where organizations have more information than can be effectively managed? How will organizations separate the meaningful information that is actionable from the disparate and fragmented information that may not be useful in the current context? As information sharing matures in communities, some questions that will need to be addressed include:

- What mechanisms are in place within the community to share information about cyber security events?
- What mechanisms are in place to do an analysis of the cyber security information? Is there a mechanism to validate or verify the information?
- What fusion is performed between cyber and physical security information that can create meaningful information?
- What distribution methods are in place and who should receive cyber-related information?

8.3.1.3 Policy

This dimension addresses the need to integrate cyber elements into the policies or guiding principles for not only organizations but also jurisdictions. The Policy dimension includes all guiding regulations, laws, rules, and documents that govern the daily operation of the community. Here, the goal is to ensure community-wide policies that affect organizations has been evaluated to include where appropriate cyber issues. This will be a progressive process as it would be an overwhelming task to have every organization (large, mid-size, and small businesses) assessed. The organizations that should have their policies assessed first are the critical infrastructures and local government to include law enforcement. Next should be the largest organizations in the community and those that may have a large impact on the community. Eventually, all organizations including the smallest businesses will be included. The policies should reflect the approaches a community intends to use during normal business operations and in the event of a cyber incident. Every policy must be looked at to see if cyber issues have been addressed specifically. For example, city government may have a policy to operate with secure and resilient business practices. The processes and procedures supporting this policy should be analyzed to ensure all new technologies used on city networks have been identified and incorporated. In addition, the city government may decide to add a minimum cyber security health standard for all vendors or partners who use the city network. Social media is a new cyber-related tool used to provide information to the general public. These policies should be analyzed to ensure that social media practices have been included. Additionally, other cyber-specific policies may need to be developed to cover cyber issues not addressed in other established policies. Policy related questions include:

- What policies are in place in various organizations within the community to address cyber security?
- Have community-wide policies been examined to see if they specifically address relevant cyber implications as applicable?
- Have supporting processes and procedures been examined to see if they specifically address cyber issues as appropriate?
- What testing/exercise/practice is conducted to evaluate the procedures and supporting policies that have been developed? Are they adequate?

- Who in the community should know about cyber additions to policies? Have they been trained?
- How often are policies updated to address current and emerging cyber threats? Is this time sufficient to ensure new threats are addressed in a timely manner?

8.3.1.4 Plans

The planning dimension is focused on the need to incorporate cyber into all continuity, emergency, and disaster recovery plans addressing how we will prepare, mitigate, respond to, and recover from incidents. This dimension needs to identify how cyber can impact the whole community and identify the cascading effects a cyber incident may cause. Each plan should be analyzed to identify cyber resources and actions needed and include them in the overall strategy to achieve objectives. An example would be to ensure cyber incident response teams have been established to act in the event a cyber-attack on the community occurs. Plans can include Continuity of Operations Plans (COOP), Disaster Recovery Plans (DRP), Emergency Operation Plans (EOP), and so on. Planning questions to consider include:

- To what extent is cyber considered in the community's disaster planning process?
- What incident response steps have been implemented and tested?
- Do plans include consideration of both cyber-only events as well as how cyber issues can impact other emergency situations?

8.3.2 Levels of the CCSMM

Dimensions are the areas in which we need to improve our cyber security posture, the next aspect of the model that needs to be discussed are the levels of improvement or preparedness—the level of maturity—that can be achieved.

The model identifies five levels of preparedness, or maturity, for communities and establishes the characteristics the community will display at each level. Each community begins at Level 1. This is the "Initial" level. The characteristics of a community at this level are minimal cyber awareness, minimal information sharing capabilities, few assessments or established policies and procedures, and little inclusion of cyber in the community's COOP. These characteristics are for the overall community which includes cross-sector coordination and capabilities.

Figure 8.1 shows a list of the characteristics of a community at each of the five levels in the model. A community is considered at a specific level when it at a minimum matches all of the characteristics at that level. The community may very well exhibit some characteristics found at higher levels. For example, a community

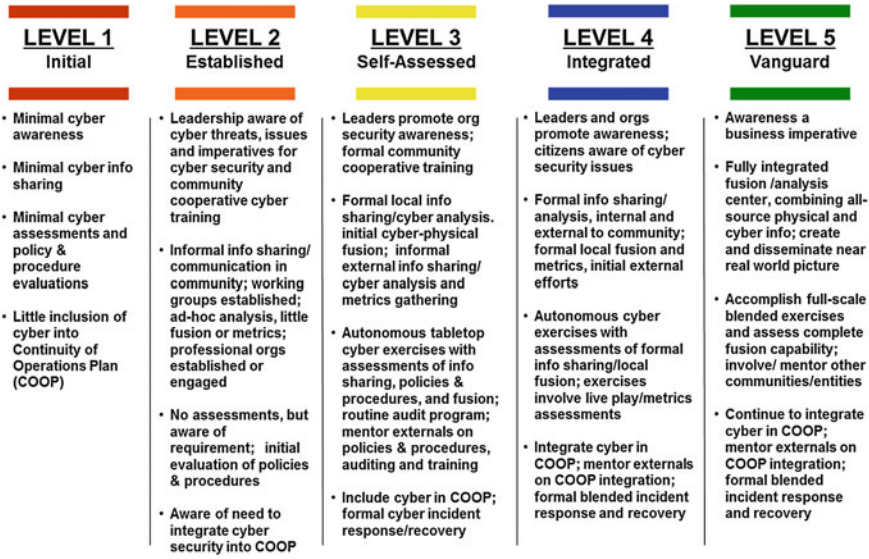


Fig. 8.1 A list of the characteristics for a community at each of the five levels in the CCSMM

that met three characteristics at level 2 and a fourth at level 3 would be considered to be at level 2 overall.

A community at level 2 has learned of the importance of cyber security and how it can impact the community and has taken steps to establish a cyber security program. The characteristics of the community at level 2, the "Established" level, include:

- Identifying leaders of the community who should be aware of cyber threats and issues that can impact the community and ensure those leaders have an understanding of the cascading effects a cyber-attack can cause.
- Informal cyber information sharing and communication capabilities within the community.
- The community may not have completed assessments for critical cyber systems but recognizes the need for this and will begin evaluating policies and procedures that should exist cross the community for cyber.
- There is an understanding that cyber should be included in the community's plans and into the COOP or other continuity plans at the community level though such inclusion may not exist at the time.

Level 3 is identified as "Self-Assessed." At this level, the community is maturing their cyber capabilities as opposed to simply recognizing the need to include cyber in the community operations. A level 3 community has:

- Leaders in the community are not only aware of the cyber threat and how it can impact the community, but are now promoting cyber security awareness

throughout the community. Formal community training cooperatives have been established to increase cyber awareness throughout the community.
- Formalized local information sharing and analysis has been implemented. Initial cyber-physical fusion of the information shared is addressed and external informal cyber information sharing, cyber analysis and metrics gathering is established.
- Testing of cyber capabilities has been established with autonomous tabletop cyber exercises and audit programs. Mentoring surrounding communities on policies and procedures, auditing and training has begun.
- Cyber elements are included in COOP plans and a formal cyber incident response program has been established. This does not mean that this capability is completely fleshed out but rather that a formal response program has been established to which new capabilities will be added as experience is gained.

The "Integrated" stage is Level 4 of the model. At this level a community-wide effort has begun to integrate cyber security considerations into all operations and activities as appropriate. This level is identified by:

- A well-established cyber awareness program for the community in which citizens and not just security professionals are also aware of the implications cyber systems have on the functioning of the community.
- A formal information sharing and analysis capability that includes both sharing of information internally within the community as well as externally with other communities and organizations. The information sharing program has been coupled with a formalized local fusion and metrics program as well. The community has begun to engage with other communities to better prepare the region or state to handle a cyber event.
- Community continuity plans have cyber security integrated into them and formal blended incident response and recovery capabilities are implemented addressing the cyber-physical relationship. A program for mentoring organizations throughout the community has been established to help those who may need help with their own cyber security maturity and this mentorship program has been extended to assist other communities on continuity plans as well.

Level 5, the "Vanguard" level, describes the most established communities who are prepared to address the most difficult cyber threats. Communities at Level 5 have the most mature cyber preparedness characteristics. At this level:

- Cyber security has become a business imperative. Cyber security is included in everything we do and is continuously updated.
- A fully integrated fusion and analysis center that includes both physical and cyber information is in place that creates a near real world picture of the actual cyber security status of the community and distributes actionable information when needed.
- Full-scale blended exercises are used to examine gaps and test capabilities of the community's response and recovery methods.

- Cyber security is considered in all COOP exercises and the community is assisting others to do the same thing in their communities.

All communities will not necessarily need to be at a level 5 state of preparedness, however, the higher the level of the community, the more prepared they will be to detect, prevent, respond to and recover from cyber threats. The ability to adapt to new threats is also much greater at the higher levels of the model.

The community's level of preparedness is only as good as its lowest dimension. It is possible to have a community at level 1 in planning and level 3 in awareness. A community such as this would be considered to be overall at level 1 for its Community Cyber Security Program.

Communities that are not to exist in isolation. They are made up of a variety of different organizations and entities and in turn are part of a larger body known as a state. In the CCSMM, each individual, organization, community, state, and other entity is evaluated along different dimensions to determine its own maturity level. The 3D version of the model depicted in Fig. 8.2 shows the relationships of preparedness for the organization, community, state, and the nation and how they are integrated together for optimum preparedness to address cyber threats. Everyone has a role in cyber security.

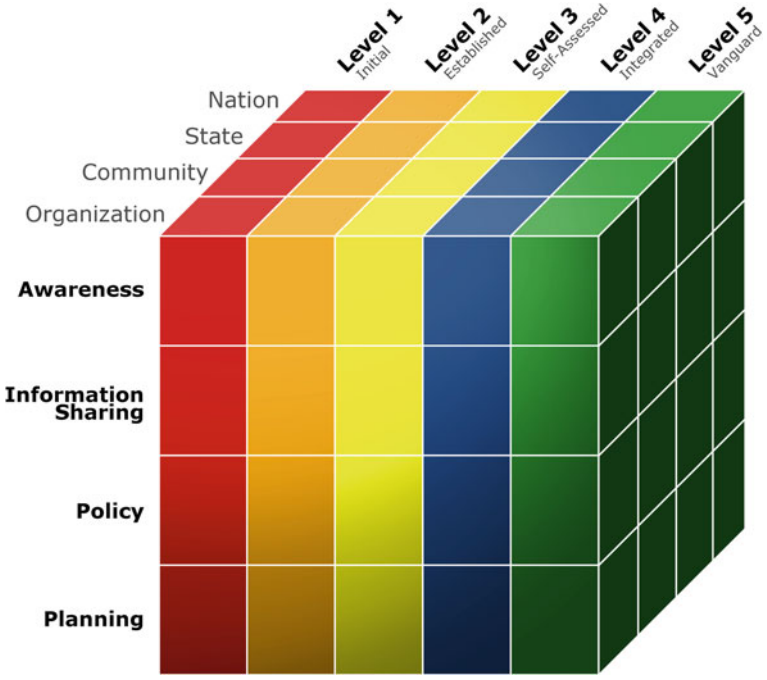


Fig. 8.2 3D version of the model of CCSMM showing the relationships of preparedness for the organization, community, state and the nation

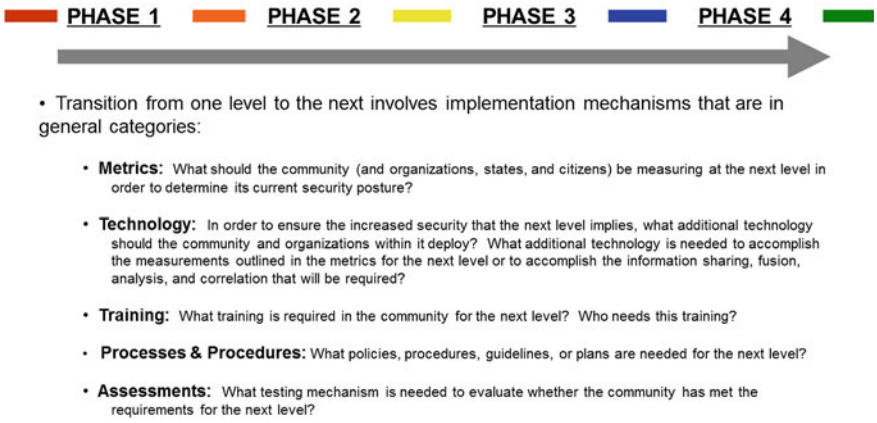


Fig. 8.3 Phases for implementation for CCSMM

8.3.3 Phases of the CCSMM

As mentioned earlier, everyone starts at level 1. There is a natural desire to progress beyond this initial state. How a community advances is described in a series of phases that helps a community to advance their level of cyber security.

A community at level 1 that wishes to progress to level 2, first must recognize that it will take a period of time to accomplish all of the work that must be accomplished to increase their level of preparedness. This period of time is called a Phase and is illustrated in Fig. 8.3.

Within the Phase period at each level, there are specific activities that need to be accomplished. Those activities are referred to as implementation mechanisms.

8.3.4 Implementation Mechanisms

Each phase contains certain implementation mechanisms. The implementation mechanisms and activities that are appropriate for an individual or organization may vary from the activities that might be appropriate for a community or state.

The implementation mechanisms, as shown in Fig. 8.3, are metrics, technology, training, processes and procedures, and assessments.

8.3.4.1 Metrics

Metrics are the measurement criteria identified that allow individuals, organizations, or the community to measure their current security posture in relation to the levels of the model. Metrics can also be used to measure the current security status of the

community in relationship to historical data indicating what normal activity is within the community. These other metrics can provide the ability to gauge whether a community (organization or state) is under attack. Similar metrics have been utilized for several years at the organizational level. Determining what is appropriate for communities, states or the nation is a more involved process. At the lowest levels of the CCSMM, these metrics mirror the ones that exist at the individual organizational level and are supplied, in a sanitized form, by the individual organizations within the community. These can then be aggregated for the community to provide an overall picture of hostile cyber activity within the community. In a similar manner, information from communities can be aggregated at the state and federal levels to provide a picture of activity within the state and nation, respectively.

8.3.4.2 Technology

Technology is obviously an integral part of any discussion on advancing the security posture of a community. Identifying the types of technology needed to prevent, detect, respond to and recover from cyber incidents will be critical. Technology will be needed to assist with assembling the volume of cyber activity data that will be available. It will be involved in how we can securely distribute information about cyber incidents and once it is obtained technology will assist in the analysis of that data to identify potential indications of intrusive activity. Understanding what technologies are available and what will work best in a community is a key factor to the success of the process. As communities mature in their cyber programs, new technologies will be needed to increase the capability of the community to accommodate the gathering and analysis of cyber security relevant data.

8.3.4.3 Processes and Procedures

To support policies created in regard to cyber preparedness, processes and procedures will be required specifically to address the step-by-step growth in the community's capability. Processes and procedures should reflect exactly how a community wants to handle cyber-related issues. To be a little more specific, what do people know about cyber-related issues and how should they handle it? What kinds of technology are used to prevent, detect, respond to and recover from a cyber-related issue and does the community have step-by-step processes and procedures on how to accomplish each? What processes and procedures are in place now and do they address all cyber-related aspects? What NEW process and procedures need to be created? How, for example, can a community detect if the community is under a coordinated cyber-attack impacting cross-sector organizations. Is there a process to communicate isolated or seemingly disparate events? Is there a process to report abnormal incidents? Who addresses cyber incidents in the

community? Is it law enforcement? A fusion center? Are there step-by-step processes that assist in identifying possible cyber incidents? Who is analyzing the information to see if this is a coordinated attack? How and when is the information provided? All of this should be incorporated into a Policy with accompanying step-by-step directions on how it will be accomplished.

Determining what policies are needed and which need to be established first can be a challenging task. The National Institute of Standards and Technology has produced the ***Framework for Improving Critical Infrastructure Cyber security*** (NIST 2014) to provide a risk-based approach to managing cyber security risk. It provides a tiered approach for organizations to advance in their own security programs in five core sets of cyber security activities. While designed to address security for critical infrastructures, the basic elements contained in this document can help to establish policies, processes, procedures, and guidelines used by states and communities in developing their cyber security programs. The tiered nature of the framework helps to blend the framework into the CCSMM.

A community should closely consider the dimensions and ensure that processes and procedures address awareness of the cyber threat. Consideration should be given to how to share information about cyber security relevant events both inside and outside the community and organizations within its boundaries and determine what policies will help address prevention, mitigation and response to cyber incidents and attacks. Processes and procedures will undoubtedly become more complex at the higher levels of the CCSMM.

8.3.4.4 Training

Training will be used to teach a needed skill, knowledge or behavior expected with cyber-related activities and incidents. Training methods are used in every aspect of the model. Any knowledge, skills or expected actions needed to address the cyber threat must to be taught to the intended audience for their specific job. Training will be used to ensure metrics are being gathered, analyzed and distributed as needed. People need to be trained on how technology works and how to execute the processes and procedures that have been developed. It is important to note that training is not a one-time effort. As new information and practices are developed and implemented, updated training needs to be developed and delivered. The methods of training will vary depending on what needs to be addressed and in what time frame. Training needs to be done in a way that addresses different groups of people and their roles specifically. Cyber awareness training as an example has not been successful when it is approached generically as an annual training for everyone. Training should be used to target particular people and what their role is specifically when it comes to cyber security. Technical training should not be given to non-technical people (i.e., individuals who do not have a need to understand the technical aspects of a system).

8.3.4.5 Assessments

Everything that is implemented to address some aspect of cyber security should be tested to ensure processes, procedures, technology and personnel work the way the appropriate plan was intended. Assessments can be technical, identifying computer and network security deficiencies, but also non-technical, determining if personnel know specific procedures to follow in a given situation. Assessments of a non-technical nature can be as simple as asking various people in the community if they know where to report a cyber security incident to within the community. Assessments of how cyber prepared we are can be accomplished in many ways: exercises, statistics, penetration testing. At each level of the model, assessments will assist to ensure that the community has identified all gaps and has incorporated updates as cyber issues change in the future.

As a summary, the areas in which a community will need to improve in order to improve their cyber security posture have been identified in the CCSMM. These areas are called dimensions and are:

- Awareness
- Information Sharing
- Policy
- Plans

There are five levels of improvement identified in the CCSMM for each of the dimensions. Additionally, the CCSMM identifies characteristics that a community should develop at each level.

As a community matures in its cyber security posture, the time it takes between levels are called phases and this is where the implementation mechanisms to improve cyber preparedness are used.

The tools or implementation mechanisms to improve are:

- Metrics
- Technology
- Policies and Procedures
- Training
- Assessments

These are the components of the CCSMM. What is needed still is an understanding of how each of these components works together. This has been accomplished by identifying a "roadmap" for communities to follow in their maturation journey.

8.3.4.6 Roadmap for Model Implementation

The CCSMM can be used as a framework to start a community cyber security program. As described in the overview, the CCSMM has three specific purposes.

The first is to measure where (how mature) the community is in its cyber security posture. The second is to provide a roadmap for what the community should be doing to improve their cyber security posture, and finally, the CCSMM provides a common reference point. The common reference point provides a way for individuals from different communities to discuss their own programs and how they have addressed the inevitable challenges associated with development of the program. The first step that needs to be taken is to determine where the community currently stands. This requires an initial assessment of the community's security posture.

8.3.4.7 Measure Current Cyber Security Posture (Initial Assessment)

Each community is unique and varies in size, assets, capabilities and many other attributes. There is, however, enough similarity in the goals of a community's security program to be able to assess where they are in their maturity of cyber security capabilities. Using the CCSMM characteristics chart (Fig. 8.1) as a guide, a community can assess what level it is currently at by analyzing each level's dimensions. The chart is an indicator of the characteristics a community has already achieved in each of the dimensions. For example, evaluating a community based on the Awareness dimension would involve determine which of the following characteristics best describes the community's current capability:

Awareness achieved:

Level 1—Minimal cyber awareness
Level 2—The leadership is aware of cyber threats, issues and imperatives for cyber security and has implemented some form of community cooperative cyber training
Level 3—Leaders promote organizational security awareness and a formal community cooperative training has been implemented
Level 4—Leaders and organizations are promoting awareness and the general-user population and/or citizens are aware of cyber security issues
Level 5—Awareness is a business imperative

Each of the dimensions will be assessed similarly. There is a possibility that some dimensions are at higher levels than others. For example, a community may find that they are at Level 3 in awareness but at Level 1 in Plans. The community is overall at the lowest level identified, in this case, they would be at a level 1.

8.3.4.8 Program Development (Building a Roadmap)

Once the level of the community has been determined, the next step is to build an action plan for the community to advance to the next level using the implementation mechanisms as shown in Fig. 8.4. A community at level 1 will build a plan to get to level 2. An example of a possible action plan using the mechanisms is as follows:

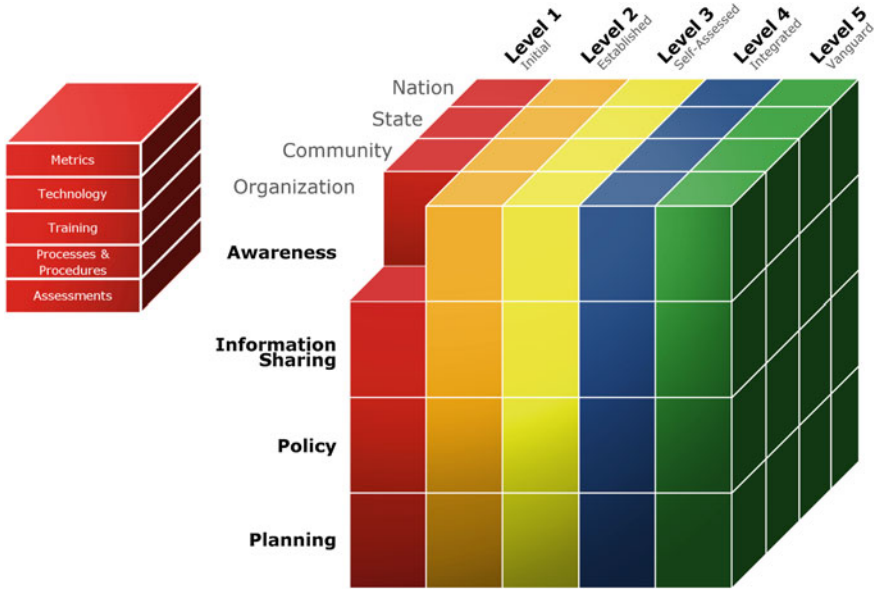


Fig. 8.4 Implementation steps for developing a community action plan

Level 1 Awareness Characteristics: minimal awareness.

Metrics:

To achieve level 2 Awareness the leadership must be aware of cyber threats, issues and imperatives and at a minimum an informal cooperative cyber training program should be in place. The community will use these measures to determine when they have achieved level 2 in this dimension.

Technology:

Webinar technology will be used to provide cooperative cyber training on current cyber security issues. This training will be made available to all community leaders. The percentage of community leaders who have taken the training will in itself provide a metric for how well the community is advancing.

Policies and Procedures:

An initial evaluation of the operational policies and procedures to find areas where cyber security should be incorporated will be completed by the end of the quarter and a report will be submitted to management.

Training:

Training on how to utilize the webinar tools is available online through the vendor. The technician will complete the training no later than the end of the month.

A one hour brief will be provided to community leadership. The briefing will contain information on the current cyber trends and issues and will include the impacts and potential implications that a cyber event in the community might have. Briefings will be conducted once a month.

Assessments:

A demo webinar will be conducted by the trained technician immediately after training is complete. A questionnaire delivered after the webinar will assess the effectiveness of the training program in making leaders aware of the potential impact a cyber security event might have on the community.

Each dimension needing improvement would go through a similar process of evaluation and planning.

Although, a community may find that there are many preparedness mechanisms it would like to address, there may not be immediate funding available to implement everything at once. There are no-cost and low-cost solutions that can be implemented immediately to start a program, allowing the community to incorporate future advancements into their budget and growth plans. For example, assessing which leaders should be aware of the cyber issues and trends; identifying which information sharing organizations exist in your community; examining community policies and plans to see if they address cyber would all be a low-cost way to start.

8.3.5 Implementation Recommendations

The best way to approach implementing a cohesive cyber security program is to implement multiple layers of security. Security is a process and cannot be bought as a single product off the shelf. The CCSMM was developed to address this process and many communities in the United States have used the model to begin the establishment of their own cyber security programs. While, each community is unique there are some implementation strategies that have been commonly used and work for the majority of communities. Other communities make minor modifications to these strategies or approaches to best match their own specific needs. The following are action plan activities that have been found to work as is or work with minor modifications.

Recommendations for approaches to advance from Level 1 to Level 2 that have been consistently used in cities across the United States:

Awareness

(1) Exercises are used from the local to national levels to test first responders' abilities to address various attacks and events. Exercises are a valuable tool in the cyber arena for the same reason. Cyber events can be introduced to communities as events in other exercises or as a cyber-only exercise. Both are important and should be part of a community's exercise and security programs. Dark Screen was the first Community Cyber Security exercise. It is a great example of what a community can do as they begin the process of building a community cyber security program. The main purpose of community cyber security exercises such as Dark Screen is to identify what is needed for all sectors to detect, prevent, respond to and recover from a

coordinated cyber-attack. A community exercise will analyze information sharing channels to evaluate how the federal, state, county and local authorities will communicate before, during and after a cyber incident. Note that for this type of exercise, a tabletop scenario was used. Most communities are at the stage where they need to first ensure everyone understands the potential for a cyber-attack—in other words most communities are in the awareness stage. They are not yet ready for a more technical type of exercise. The incidents used in an exercise at this level are not technical. The purpose of the exercise is as much awareness as it is to evaluate any plans or processes that may be in place.

(2) Identify a champion. The champion is a person in a leadership role within the community who can rally and push the cyber security program forward. Often priorities change and various agendas distract from the focus of achieving the goal. Individuals have other responsibilities and other issues within a community will require their time. The champion can get those involved in establishing the cyber security program reengaged as necessary to get back on track to reach the next level.

(3) Identify community leaders who should be aware of cyber issues. Some possibilities may be the mayor, city manager, police and fire chiefs, medical, financial, and business leaders, critical infrastructure providers, educational institutions, and media representatives. Anyone in a leadership role who makes decisions for the community or a portion of the community, should be included in the training and exercises.

(4) Explore ways to have leaders within the community become more aware of cyber issues and the potential for a cyber event to adversely impact the community. This can be challenging as leaders often do not have an abundance of time. Exploring ways to engage them and maintain their awareness level is a must as the cyber security threat is continually evolving and changing. Some recommendations for improving community leaders' awareness of cyber issues, are presentations by cyber security organizations or professionals who are members of groups such as Information Systems Security Association (ISSA); awareness courses designed to cover exactly what a leader needs to know such as return on security investments and implications of a cyber-attack; cyber security exercises with leadership involvement; leadership meetings with cyber security discussion topics; and the creation of a cyber security council or advisory group for the community leaders.

(5) Form a training working group to research and implement low- or no-cost awareness programs both within and across organizations such as posting flyers, issuing email reminders, holding lunch seminars, and recognition or awards programs. A good time to start these community-wide efforts is in October during the National Cyber security Awareness Month.

(6) Identify and use free resources for awareness programs: Stop. Think. Connect. A program from Department of Homeland Security (DHS), is a resource that should be examined.

Information Sharing

(1) Create working groups to examine interdependencies throughout the community and information sharing mechanisms that could be used.
(2) Discuss cyber information sharing issues from the local level with the state and federal entities. For example: will the state provide resources during or after a cyber-attack and at what point can officials at the local level request assistance and how is that request executed?
(3) Information sharing is critical for timely responses to cyber events that can have a devastating impact in seconds. Methods to facilitate the timely sharing of information and response to cyber events in the local community need to be established. Form a working group to find methods to share information cross-sector within the community. Take advantage of groups such as the FBI sponsored InfraGard program and other security-related professionals' organizations where they exist.
(4) Create a contact list of security professionals and points of contact within the community and have a backup list that is not digital. This list should be tested periodically to ensure it is current and that change with community contacts is documented.
(5) Establish clear thresholds for when and how to share information about cyber security incidents based on what is normal for the organization or community. The first step is for each organization to create a baseline of what is normal for them.
(6) Develop processes to accomplish bidirectional information sharing that effectively accommodate receiving information as well as transmitting it, and ensure that these processes take into account external reporting requirements and laws. Processes should be developed within participating organizations and extended into the community.

Policy

(1) Create and implement cyber security policies where there are none. Improve or update cyber security policies where needed. Review and/or create policies to address specific cyber events that might be experienced.
(2) City and county officials might also consider establishing a cyber security advisory panel consisting of members from government, academia, and industry to help guide local policy decisions relating to city/county cyber security preparations.
(3) Work with the state to develop state processes, procedures, and guidelines for communities to address cyber security incidents. This occurs in other areas such as when the state assists communities during natural disasters—how will the state assist during cyber events?
(4) Specify policy life cycles to ensure the continued applicability and relevancy of the policy. Assign this to a person or persons who can own the process.

(5) Review existing policies to identify barriers to cyber security goals and determine if the barriers are real or perceived, and if and how they can be worked around.
(6) Ensure that policies are simple and easy to understand to promote individual ownership of cyber security. Training of all new policies must be completed in a timely fashion—no more than 30 days from the implementation date.
(7) Ensure that policy is compliant with any and all applicable laws.

Plans

(1) A city Computer Emergency Response Team (CERT) should be created that could address cyber security events for the city and the surrounding area. The CERT membership should consist of individuals from local government, academia, and industry.
(2) Create an advisory group on cyber issues for the community and address how they are integrated into continuity of operations.
(3) Involve key organizational stakeholders, such as executive-level management, legal departments, and communications groups, as early as possible in planning processes.
(4) Create or continue exercise programs that address cyber and cyber/physical issues, vulnerabilities, and response options.
(5) Identify all cyber security improvement plans needing cyber security to be integrated into them. Plans such as EOP, Standard Operating Procedures (SOP), COOP, and other existing improvement plans.
(6) Utilize readily available templates for policies and procedures from free online sources such as the Escal Institute of Advanced Technologies (SANS Institute), the National Institute of Standards and Technology (NIST), or the Multi-State Information Sharing and Analysis Center (ISAC).
(7) Research no/low-cost government and nonprofit training resources, such as DHS-Federal Emergency Management Agency (FEMA), various universities, NIST and the National Cyber security Preparedness Consortium (NCPC).

Once characteristics have been achieved at the goal level. The process may begin again to develop plans to reach the next level of maturity if the community has decided it is needed. Periodic assessment of the characteristics at the lower levels should be done to ensure the dimensions are maintained.

8.4 Summary

It is increasingly becoming important for states and communities to prepare for cyber incidents that might adversely impact them. There have been numerous documented cases where a city has experienced a loss from a cyber-related incident. The vast majority of communities are not prepared for even the smallest of cyber security incidents. Few have any established cyber security program. Most fear

starting one because of the potential cost and the fact that they may simply not know where to start.

The CCSMM provides an easy entry point for communities who want to start on the development of their cyber security program. It provides a ready approach for starting, and maturing, a community's cyber security program. It begins with relatively easy steps that also have a minimal cost, if any, associated with them. There are a number of cyber preparedness resources available to assist communities and organizations. The key is to identify and engage in a program to detect, prevent, respond to and recover from cyber incidents efficiently and effectively BEFORE the community experiences a cyber event.

References

Barron, J. (2003, August 15). The blackout of 2003: The overview. The New York Times.

Enbysk, L. (2015, July 24). Cities at risk: 5 that were victims of cyber attacks. SmartCitiesCouncil.com. http://smartcitiescouncil.com/article/cities-risk-5-were-victims-cyber-attacks

Goles, T., White, G. B., & Dietrich, G. (2005, June) Dark screen: An exercise in cyber security. *MIS Quarterly Executive, 4*(2).

NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, National Institute of Standards and Technology, February 12, 2014, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

Presidential Policy Directive 8: National Preparedness, March 30, 2011. Obtained February 2, 2016 from http://www.dhs.gov/presidential-policy-directive-8-national-preparedness

White, G., & Sanchez, J. (2003, January) Dark screen sheds light on cyberspace security issues. *Signal Magazine.*

Chapter 9
Fighting Cybercrime: A Joint Effort

S. Boes and E.R. Leukfeldt

Abstract This chapter describes the fight against cybercrime from a European perspective. Law enforcement agencies always have had an important role when it comes to fighting crime. However, in this digital era, several problems hamper the effectiveness of the police combating crime. Therefore, the first part of this chapter describes the difficulties the police have in fighting cybercrime. The second part of the chapter focuses on one of the strategies to overcome some of these difficulties, namely forming alliances with private institutes. This joint-up approach is mostly realized by public–private partnerships (PPPs), consisting of formalized cooperation between governmental authorities and important stakeholders. Cooperation between governmental and private actors is no sinecure, as will appear from a public administration perspective. Successful cooperation depends on several factors, which will be theoretically described and practically illustrated. Conclusively, the discussion paragraph handles the common dilemma of the extent to which the government should play a leading role in the fight against (cyber) crime.

Acronyms

CERT	Computer and Emergency Response Team
CPNI	Centre for Protection of the National Infrastructure
DDoS	Distributed Denial of Service
ECTF	Electronic Crimes Task Force
ENISA	European Network and Information Security Agency

S. Boes (✉) · E.R. Leukfeldt
Cyber Safety Research Group of the NHL University of Applied Sciences, Leeuwarden, The Netherlands
e-mail: s.boes@nhl.nl

E.R. Leukfeldt
e-mail: e.r.leukfeldt@nhl.nl

S. Boes · E.R. Leukfeldt
Police Academy, Apeldoorn, The Netherlands

S. Boes · E.R. Leukfeldt
Open University, Heerlen, The Netherlands

R.M. Clark and S. Hakim (eds.), *Cyber-Physical Security*,
Protecting Critical Infrastructure 3, DOI 10.1007/978-3-319-32824-9_9

GOVCERT	Government Computer Emergency Response Teams
IP	Internet Protocol
ISAC	Information Sharing and Analysis Center
ISP	Internet Service Provider
NCSC	National Cyber Security Centre
NPM	New Public Management
NSP	National Skimming Point
PPP	Public–Private Partnership
SME	Small and Medium-sized Enterprise

9.1 Introduction

Safety is a public good, which can be threatened by crime. Nowadays, not only safety in the offline world but also safety in cyberspace is a value that should be guaranteed. Regarding the fact that public authorities have difficulties with taking care of safety in the 'real world', it is not hard to imagine that this also applies to cyberspace. Wall (2007) even questions the traditional local dominance of the police over the cyber security domain. He states that the role of the public police in fact could be marginalized completely. As Jewkes and Yar (2008:582) note: "*The scope, scale and structure of the internet outstrops the capacity of any single enforcement of regulatory body.*" The monitoring, regulation, protection, and enforcement related to cybercrimes are not solely responsibilities of state-controlled public police. This stresses the need for alternative strategies to cope with the policing deficit. A possible strategy to overcome such problems is an integral approach, which is an approach wherein all relevant stakeholders—public as well as private—participate in (the implementation of) safety and security policy. An outgrowth of such an integral approach is a public–private partnership (PPP).

The integral approach can be illustrated with a so-called soccer model (Boutellier 2005). Considering fighting crime as team play, Boutellier (2005) introduced the soccer metaphor to describe the position of the different actors involved in safety. In this model, there are three different kinds of players. First, civilians play a role in the front line by, for example, acting safely, taking preventive measures, signalizing problems, and exercising social control. The midfield consists of institutions whose primary goal is not safety, but which nevertheless have a function within the scope of safety. Such institutions include schools or housing cooperatives. Finally, the line of defense is formed of institutions whose task is primarily safety related, e.g., police, prosecutors, or private security companies.

Regarding cybercrime, the playing field is as follows. First, end users play a role in the front line. They should secure their own computers, for example, by installing and keeping up-to-date virus scanners and fire walls. Furthermore, end users need to think consciously about their online activities (e.g., about the type of personal information they share online through social media and the type of web sites they

download from). In this way, the end users not only protect their own computer, but they can, for example, also prevent that their computer becomes part of a botnet used by criminals to commit other forms of cybercrime.

The midfield consists of institutions whose primary goal is not safety in cyberspace, but which nevertheless have a function within the scope of online safety. Examples include Internet Service Providers (ISPs), manufacturers of hardware and software and Internet hotlines (e.g., Internet Crime Complaint Center and International Association of Internet Hotline). ISPs play an important role, since they provide access to the Internet to individual users and businesses.

Finally, the line of defense is formed of institutions whose tasks are primarily safety related, e.g., police, prosecutors, or private security companies. Important players are commercial cyber security companies (selling virus scanners to end users or protecting vital ICT infrastructures of business) and law enforcement agencies.

This chapter focuses on this integral approach of the fight against cybercrime from a European c.q. Dutch perspective. It gives an overview of the state of affairs in scientific literature as well as Dutch practice in this respect. First, we shortly describe the role of the police—as they are still seen as one of the major actors in the fight against (cyber) crime—and the problems they encounter in the fight against cybercrime. Thereafter, this chapter focuses on PPPs. First, PPPs will be discussed from a public administration perspective, including topics such as definition and appearance, theoretical assumptions, and success and failure factors of PPPs. In addition, a Dutch public–private partnership established within the field of cybercrime will be described in-depth. Finally, this chapter ends with a discussion paragraph which addresses the debate about the sharing of responsibilities between the different parties involved in safety.

9.2 Problems in Policing Cybercrimes

In this paragraph, we will address the problems the police encounter in combating cybercrimes. Academics observe time and again that the police and the courts are unable to stay abreast of developments on the Internet and are behind the times, notably in cases of more or less everyday cybercrimes that do not fall within the remit of specialized national police units (Jewkes and Yar 2008; Van der Hulst and Neve 2008; Leukfeldt et al. 2010; Stol et al. 2013; Struiksma et al. 2012).

9.2.1 Problems Policing Cybercrimes in General

Several studies show that law enforcement agencies—except some specialist cybercrime teams—have a lack of knowledge about what is exactly happening on the Internet with regard to crime and how that can be detected—despite the priority

given to cybercrime in recent years (Bossler and Holt 2012; Gogolin and Jones 2010; Holt and Bossler 2012; Hunton 2011; Jewkes and Yar 2008; Jewkes and Leukfeldt 2012; Leukfeldt et al. 2013a). A major problem linking to this is the rapid innovation cycle of cybercrimes, which ensures a continuous supply of new technologies and tools to commit crimes (Koops 2010).

The above implies that the probability of detection is low. Zhang et al. (2007) studied informal sanctions, formal punishment, and perceived probability of detection of hackers, and showed that both informal sanctions and the perceived risk of being caught are seen as low by hackers themselves. Consequently, the deterrent effect of punishment for this crime is low. The researchers attribute the low probability of detection to the anonymity in which hackers (think to) operate and the lack of control on the Internet. To carry out their criminal acts, criminals have to remain out of sight of the police. However, just like in the real world cybercriminals leave (digital) traces. Each communication over the Internet, for example, contains the IP address of the sender and receiver. To reduce the chance of getting caught, criminals conceal their identities, take on false digital identities and/or cover their tracks. The Internet offers plenty of opportunities here. An IP address can be disguised using anonymizers or IP spoofing, encryption can be used to hide information (Koops 2010). To join forums on which cybercriminals sell their tools and expertise, the use of encryption, secure Internet connections, and other preventive measures are obligated (see, e.g., Stol et al. 2008, 2009; Soudijn and Zegers 2012). These technological measures complicate the identification of potential suspects and the gathering of evidence, and give criminals an easy way to enjoy a degree of (perceived) anonymity.

In addition, the police struggle with the international nature of cybercrime. Due to the international nature of the Internet, crimes committed via the Internet have international components very quickly (e.g., a criminal who infected a web site from country x in country y steals the identity of someone in country z). There are also digital offender convergence settings such as forums where stolen identities are traded, where criminals from all over the world can meet each other, search for other criminals with the right expertise, plan new activities, purchase or sell tools, and exchange knowledge (Peretti 2008; Holt and Lampke 2009; Lu et al. 2010; Soudijn and Zegers 2012; Soudijn and Monsma 2012; Decary-Hetu and Dupont 2012; Yip et al. 2012). These digital offender convergence settings offer—more than in the offline world—possibilities for fluid transnational networks.

All of this has implications for the investigation and prosecution of cybercriminals. Needless to say, international cooperation is complicated and time consuming. However, more important is that—just as with traditional crimes—a significant part of the cybercrimes that must be dealt with should be taken up by (inter) regional teams (Stol et al. 2013; Leukfeldt et al. 2013b). Furthermore, there is little case law and, despite international conventions, there are still differences in legislation between countries (Wall 1997; Grabosky 2000, 2001; Capeller 2001; Koops 2010). Criminals can therefore move to countries where legislation related to cybercrime is outdated or nonexisting.

9.2.2 Case Study: The Netherlands[1]

In the Netherlands, the so-called basic police units investigate everyday crime. With the advent of cyberspace, the fight against cybercrime, such as fraud or extortion via the Internet, is now also part of the basic units' workload. These units consist of police employees without specialist knowledge of cybercrime. The research results presented here refer to basic police units that have to deal with everyday (cyber) crime cases.

A first problem in detecting and investigating cybercrime lies in the fact that victims of cybercrime do not always notice that they are being victimized. In addition, a self-report study in the Netherlands shows that merely 13.4 % of the victims report cybercrime to the police (Domenie et al. 2013). In addition, a self-report study into victimization of SMEs shows that 7.2 % of these reports cybercrime to the police (Veenstra et al. 2014). Subsequently, if victims do report cybercrime to the police, it is unsure whether the police will register the report. Interviews and earlier research suggest that police employees who are responsible for registration—which forms the basis of the criminal investigation process—have a lack of knowledge about cybercrime. As a result, they sometimes do not register cybercrimes and if they do, they are unable to register these offenses properly (Toutenhoofd-Visser et al. 2009). Therefore, the first problem in the fight against cybercrime is that a significant part of cybercrimes will never enter the criminal justice system.

Once a crime has been registered, a screening process starts. A so-called case screener of the police checks to what extent the report includes keystones for criminal investigation. In the interviews, respondents repeatedly state that police reports about cybercrime cases lack such keystones, because of the deficit in knowledge of police employees in the registration process. As a result, these cybercrime cases will not lead to further investigation and flow out of the criminal justice process early. Cybercrime cases that pass the screening are sent to teams of criminal investigators (not being cybercrime specialists). Due to scarce capacity, criminal investigators cannot handle all incoming cases. Therefore, the work offered to them is prioritized. Despite the fact that the Dutch government gives priority to cybercrime, criminal investigators consider cyber cases as inferior to 'traditional' crimes. Respondents state that three main reasons underlie this observation: (1) the (social) impact of cybercrime is lower than the impact of traditional crime; (2) criminal investigators have a lack of experience regarding cybercrimes; and (3) they have too little knowledge to effectively investigate these cases. Then by definition scarce amount of criminal investigators therefore prefer to handle traditional crimes. The unwanted consequence is that cybercrime cases are not investigated, not prosecuted, and thus not adjudicated. The police recognize the problems mentioned and have several strategies to overcome these problems, such as

[1]This section is based on Leukfeldt et al. (2013a, b) and Veenstra et al. (2014), studies which describe the functioning of law enforcement agencies when handling cybercrimes.

education of police personnel or the development of good practice guides by means of research. Another possible strategy is to involve others in the combating of cybercrime by means of PPPs, which is the focus of this chapter.

9.3 Public–Private Partnership

As stated above, forming PPPs might help to reduce problems which the traditional public police encounter. This counts for traditional crime as well as cybercrime. Alliances between government and private stakeholders received massive attention of criminologists and scholars from the public administration discipline. This paragraph uses a public administration perspective from which topics such as definition and appearance, theoretical assumptions, and success and failure factors of PPPs will be discussed. The choice for this discipline is quite obvious. Since a PPP has the characteristics of a multiagency approach (Hoogenboom and Muller 2002), the public administration literature can provide guidances for the formation and acting of PPPs.

9.3.1 What Makes a PPP?

Brinkerhoff and Brinkerhoff (2011) identify an 'analytic cacophony related to PPP', which is due to, amongst others, a myriad of arguments based on either empirical evidence or political rhetoric. Therefore, it is difficult to distinguish reality from storytelling. As a result of the massive attention of public administration scholars, there are a lot of definitions of PPPs (Brinkerhoff and Brinkerhoff 2011). However, not every definition is equally useful since an important part of this literature relates to alliances between governmental agencies and private stakeholders regarding subjects such as infrastructure, building projects, etc. A definition that contains elements which could apply to cooperation in respect to handling the problem of crime is formulated by Heldeweg and Sanders (2011:34), who describe a PPP as "*a judicially structured collaboration between one or more governments and one or more private corporations that aims to develop and carry out a joint strategy in order to realize a policy project.*"

The term public–private partnership consists of a classic dichotomy, namely public and private. These concepts refer to the status of different institutions. The definition of these concepts is very ambiguous, since the difference between these can be based on several characteristics of the institutions, e.g., legal form, tasks and activities, or values to aim at (Van Montfort 2008). In general, public actors are governmental actors, all other actors are private organizations. A characteristic of a public actor is that its aim should be looking after the public interest, but there is no consensus about the definition of 'looking after the public interest'. However, a general characteristic in all definitions is that public actors should not look after interests of individuals or groups in particular, but of society as a whole (Smit

2010). Providing safety in society means regulating behavior and disposing social relationships. Therefore, it relates to social and public values which go along with setting standards about right and wrong, and thus about (de) criminalization of behaviors, as well as about identifying risk groups and situations (Terpstra 2011). Thus, providing safety is not only a private value, but also a public value and should therefore be carried out with great care: arbitrariness and opaqueness are undesirable (Terpstra 2011). As a result, it is not self-evident that private institutions are involved in the guaranteeing of safety as a public interest.

Providing safety in society requires crime fighting. Crime is a problem of society, which is traditionally handled by public authorities. These kind of social issues have their own dynamics and characteristics. They are very complex, they are constant subject to changing circumstances and there are ambiguous assumptions about the right solution(s) (Rittel and Webber 1973). Van Delden (2009) enumerates several characteristics of problems the public sector has to deal with. Societal problems mostly have a normative connotation and are subject to the delusion of the day. They can also be characterized as multidimensional: problems address several aspects of society and the solution thus requires the involvement of several actors. Moreover, several problems engage in each other and are ambiguous. Situations constantly change and therefore a chosen approach can quickly become outdated. Van Delden furthermore states that every solution often is the herald of a new problem, which could have a reducing effect on the solution to the initial problem. Moreover, social problems have, by definition, an unlimited reach, so every moment new fields and actors can come into view. Herein, technology plays an important role: it increases this boundlessness. Thus, in spite of the action perspectives technology offers, it makes problems far more complex. The complexity of this kind of problems stresses the need to involve stakeholders in the solution of those, and thus the relevance of PPPs.

9.3.2 Forms of PPPs

There are several ideas behind the extra value of forming public–private partnerships. The basic assumption is that this extra value of public–private partnerships might be obtained by combining knowledge and coproduction (Klijn et al. 2008). Klijn and Van Twist (2007) distinguish two different bodies of knowledge behind that supposition. The first can be found in the idea of New Public Management (NPM): government formulates policy, others should carry out this policy. Osborne and Gaebler (1992) used a 'rowing and steering metaphor' to express this idea: government should steer, while other actors should row. The assumption is that this strategy raises effectiveness and efficiency. The second body of knowledge defines PPPs in terms of 'the shift from government to governance'. Governance is based on the assumption that a better horizontal coordination leads to better products, more innovation, and easier ways to carry out policies. From this point of view, actors are more interdependent and stress the need of interorganizational

coordination, and sharing information, knowledge and resources (Klijn and Van Twist 2007). Resultantly, two main models can be derived from the public management literature, describing the different forms in which government 'makes use' of private actors, namely a concession model and a partnership model (Hodge and Greve 2005; Klijn et al. 2008).

The construct of the concession model, which can be described as 'smart procurement' (Van Montfort 2008), is mainly applicable in the field of infrastructure and investment projects, etc. In the safety domain, this form of PPP mainly exists in the sphere of prevention, such as hiring private security personnel. The government formulates a problem and needs a private actor to solve it. In such cases, there is a hierarchical client—contractor relationship. The second model is the partnership model or 'smart cooperation' (Van Montfort 2008). Public and private actors jointly formulate a problem and jointly seek for a solution. In such cooperation, sharing knowledge and capacities is important. A covenant is mostly used to formalize the cooperation. Such a covenant can be described as a "*written agreement to cooperate and a frequently used means of recording the most important tasks and responsibilities, such as the goals and results to be achieved, and the manner of information sharing between the actors involved*" (Schuilenburg 2012:11). Furthermore, the relations between the cooperating actors are less hierarchical than in the first model. Mutual trust plays a more important role, and efficiency and reducing costs are of minor importance compared to the contract model (Van Montfort et al. 2012).

Additionally, Heldeweg and Sanders (2011) distinguish the partnership model in two forms, namely network PPP and authority PPP. Network PPP implies a joint establishing of goals, but the parties involved have different responsibilities. Governmental actors lay down compulsory policy and the private parties involved can at most contribute to its implementation. Authority PPP is one step beyond, therein private parties are not only involved in formulating joint goals, but also in establishing policy and making decisions which might be judicially binding for citizens. The difference between these two forms of the participation model is caused by the exercise of public authority and makes an authority PPP fundamentally different from network PPP: private actors also (have to) serve the representation of the public interest and might affect the legal positions of civilians (Heldeweg and Sanders 2011).

However, cooperation by means of a PPP is no sinecure. The differences between public and private organizations, for example, cultural differences and opposite interests, could hamper cooperation. In order to achieve a successful PPP, there are several success and failure factors which could be derived from the scholarly literature.

9.3.3 Success and Failure Factors

This paragraph discusses good and bad practices for PPPs in general. Indeed, cooperation between government and other parties in offline safety does not

fundamentally differ from cooperation on behalf of cybercrime. However, there are some cyber specific lessons learned from cooperation in cybercrime cases. This paragraph concludes with these lessons.

Private actors can contribute to partnerships in several ways. Roughly, cooperation consists of the sharing of information and expertise, coordinated action and the deployment of people. Usually, there is a combination of several kinds of contribution (Visser et al. 2008). However, it is rather impossible to list all factors contributing to successful cooperation, since the effect of factors depends on the cooperation form, the goal, the context, and the character of the actors involved (Van Montfort et al. 2012). Nevertheless, the following enumeration, derived from scientific literature, lists some factors which appear to be relevant in several partnerships.

First, there should be a clearly defined goal (Schuilenburg 2012). The goal and the objectives need to be clear to all partners, and should be realistically capable of attainment. According to Hudson et al. (1999), goals which lack clarity or attainability will diminish collaborative enthusiasm. A clear problem analysis, a shared problem vision along with a sense of urgency and similar goals of the cooperating parties are also crucial (Boonstra 2007; Hudson et al. 1999; Terpstra and Kouwenhoven 2004). Therefore, a shared vision (Hudson et al. 1999; Visser et al. 2008), an agreed mission and strategy are required (Hudson et al. 1999). Thereby, a success factor is the involvement of actors which are part of the problem (Boonstra 2007).

Second, it is important to determine the added value of cooperation. Thus, there must be recognition of the need to collaborate. This requires shared interests as well as mutual dependency. It means that there should be a real problem for all cooperating partners, which should be solved according to all these parties. Besides, the actors must be interdependent for a solution (Visser et al. 2008). This is well illustrated with the establishment of the Dutch National Skimming Point (see text box 9.1 below).

Box 9.1 National Skimming Point (Hagenaars and Bonnes 2014)
The amount of damage in 2009 in the Netherlands (36 million euros) was the reason for the banking sector to undertake action by means of a task force skimming. Skimming is the illegal obtaining and copying of debit and credit card information. At first, the demand for cooperation and information sharing with the police was not heard. All parties recognized the need for cooperation between the public and the private sectors, but none of these were prepared to take the lead. A lack of capacity and priority were the main bottlenecks. In the end, a regional police force was willing to take the initiative and to participate in a programmatic approach together with the banking sector and the national prosecution services. It resulted in the National Skimming Point (NSP) which serves as a national information and expertise center for the police and criminal prosecution authority. The NSP receives, processes, and provides information at an operational level. They also analyze information for tactical and strategic purposes and disseminate knowledge and expertise.

Third, it is also important to acknowledge areas of independence, meaning those activities which organizations define as their field of expertise (Hudson et al. 1999). Therefore, an important aspect in the forming of a cooperation arrangement is the division of tasks and responsibilities of the several organizations as well as the recording of it.

Fourth, there should be clarity about the financial resources of the cooperative (Schuilenburg 2012). Some pressure from the environment is important, e.g., political support might facilitate mobilizing resources. Resources consist not only of money, but also sufficient capacity—manpower, means, material, and time—is essential (Visser et al. 2008).

Fifth, optimal information sharing is important (Schuilenburg 2012). According to Bekkers et al. (2006), this information sharing between governmental agencies and private actors should be fast, whereby it is not only about sharing intelligence and information about crime suspects, activities, objects, and possible consequences, but also about sharing knowledge and experiences. Private actors might possess a lot of knowledge, experience, and information, e.g., because they are owner or administrator of a certain vital infrastructure. Exchanging experiences and shearing lessons learned with all parties involved and/or stakeholders might help prevent future incidents. An important condition is mutual trust (Schuilenburg 2012; Visser et al. 2008). Mutual trust and informal, personal contacts play an important role in sharing and exchanging information. Since hidden agendas are odious, transparency about the motives and considerations of all parties involved is vital (Visser et al. 2008). A good example of the importance of information sharing and mutual trust is offered by a Dutch PPP, namely the Electronic Crimes Task Force (see text box 9.2).

Box 9.2 Electronic Crimes Task Force (Hagenaars and Bonnes 2014)
The Electronic Crimes Task Force (ECTF) consists of cooperation between the banking sector and the criminal justice authorities regarding advanced online banking fraud, which undermines the integrity of the financial system. This PPP is supposed to bring information about banking fraud from several stakeholders together on an operation level, in order to prepare criminal investigations. Participants are the National Unit of the Dutch Police, the criminal prosecution service, the Centre for Protection of the National Infrastructure[2] (CPNI), the Dutch Banking Association and several major banks. The ECTF focuses on the so-called three I's: Intelligence, Interventions, and Investigations. This means strengthening of the information position, preventive and repressive measures such as thresholds and barriers, and investigation and prosecution of suspects and criminal organizations, respectively. The ECTF invests in sharing information and the

[2]Nowadays, CPNI is part of the Dutch National Cyber Security Centre (NCSC).

enrichment to intelligence. Some successful interventions consist of measures against money mules, the taking down of several phishing sites, and the investigation of several cases.

In general, it could be stated that trust, knowledge, communication, and the ability to cooperate are the main factors (Boonstra 2007). The success factors mentioned above count for public–private partnerships in general. Additionally, actual cyber incidents also provide good practices. The case of *Diginotar*, in which certificates were stolen from a major Dutch registrar, is such an incident. Text box 9.3 offers more information about this incident.

Box 9.3 The Diginotar Incident (Dutch Research Council for Safety [in Dutch: voor Veiligheid] 2012)
Diginotar was a company delivering digital certificates intended for the protection of electronic communication with and between governmental institutions. The Dutch government guaranteed the reliability of the certificates. In 2011, the computer system of Diginotar was hacked. As a result, the servers on which processes for certification services took place could be entered and the keys which validate these certificates as a proof of their authenticity could be abused. The hacker generated at least 531 false certificates. Only a small part of these were brought into circulation. After the hack, the Dutch government could no longer guarantee the safety of communication between governmental authorities and civilians and businesses.

The incident presented above resulted in close cooperation between government, industries, and the scientific community within the Dutch Government Computer Emergency Response Teams (GOVCERT.NL). Van den Heuvel and Klein Baltink (2014) enumerate several lessons that could be derived from this incident. First, mutual trust can be built from the actual experience of cooperation and dialogue and confidence is enhanced by reputation. Second, taboos are taboo. Sensitive topics must be openly discussed within organizations and within society, since incidents will become public anyway. Therefore, openness will enhance reputation. Thereafter, cyber security is equivalent to economic security and should be determined in terms of economic benefits. Fifth, organizations should also focus on detection and on a multidisciplinary response, since ICT and technical security measures are not consummate. Besides, learning from incidents is important. Lessons learned from the different stages of an incident should be discussed and conveyed, not only inside but also outside the cyber security community. Finally, the moral capital to incidents should be emphasized. This addresses the responsibility of the managerial level in taking care of cyber security before, during, and after incidents (Van den Heuvel and Klein Baltink 2014:129). "*Do not try to hide it*

from the public, but take an active approach to communicate what went wrong and inform the public about the things that will be changed to prevent similar incidents in the future" (Hoogenboom, in: Van den Heuvel and Klein Baltink 2014).

The reverse of preconditions consists of failure factors. The functioning of a PPP may be hampered because of different views on the approach. An informal intercourse between persons involved in a PPP could improve the decisiveness and purposefulness of a cooperative, but might also cause vulnerability, for example, when the effective execution of functions depends on the employed person. Furthermore, the intern policy of a participating actor can conflict with the policy of the PPP (Terpstra and Kouwenhoven 2004). Visser et al. (2008) state that problems within the cooperating organizations can hinder a PPP as a whole. They also state that it is important that not only the working floor or not only the management level take part in the PPP, but both of them; both levels should recognize the importance of it (Visser et al. 2008).

In general, Boonstra (2007) states that the differences between the cooperating actors are mostly considered as failure factors that obstruct cooperation. These differences can relate to, e.g., goals, methods, cultures, expectations, or interests. However, just these differences between the parties involved are the main reasons to start a joined approach. Therefore, Boonstra (2007) ascertains that the risk of a failing cooperation is not due to the differences between the parties involved, but to the inability to cope with these differences.

9.4 PPP Practice—The National Cyber Security Centre

Cooperation between public and private actors when handling cyber security threats is a widely used strategy in Europe and elsewhere. According to the European Network and Information Security Agency (ENISA[3] 2011), a threefold distinction can be made when studying the variety cooperating forms, namely 'prevention focused', 'response focused', and 'umbrella' PPPs. These terms refer to the moment of intervention of the operation, namely proactive, reactive, or both. In this section, an example of a Dutch umbrella PPP, the National Cyber Security Centre (NCSC), will be described. Several countries, including the United States, have comparable umbrella PPPs, consisting of public and private stakeholders and responsible for the protection of critical infrastructures (ENISA 2011).

The Dutch NCSC has been in existence since 2012 and builds on the former GOVCERT.NL, the organization charged with cyber security and incident responses from 2002 until 2011. NCSC focuses on monitoring, knowledge exchange, prevention, and incident handling. Besides the NCSC, a Cyber Security Council with members from industry, government, and academia was established.

[3]ENISA is an agency of the European Union, serving as expertise center for the European Union Member States and European institutions.

The NCSC aims to increase the resilience of the Dutch society in the digital domain by means of a joint approach. The NCSC wants to achieve a resilient society by, first, gathering information and expertise from government, businesses, universities, and international contacts. This contains information, practical knowledge and experiences, and knowledge derived from scientific research. The NCSC analyses this data and identifies threats, gives insight in a possible approach to threats and gives possible solutions for problems. Second, the insight in threats creates possibilities to develop measures in order to counteract the caused damage. In case of an acute threat, the NCSC plays an alerting role, so that parties involved can prepare themselves. Third, the NCSC can strengthen in cases of a crisis situation by means of functioning as coordinating spindle (NCSC s.d.). Concrete measures regarding the resilience of society consist for instance of awakening campaigns, such as 'Alert Online', 'Banking data and login details. Keep them secret' (*in Dutch*: 'Bankgegevens en inlogcodes. Houd ze geheim') en 'Protect your company' (*in Dutch*: 'Bescherm je bedrijf'). Furthermore, a guideline for responsible disclosure policy has been formulated, which provides organizations with directions for the announcement and handling of vulnerabilities of information systems and software in a responsible manner. Since its implementation, about 40 organizations, for example, financial institutions and the telecom sector, implemented a responsible disclosure policy (NCSC 2014).

In order to achieve its objectives, the Centre is developing three public–private networks (Van den Heuvel and Klein Baltink 2014). The first is a national detection network. This facilitates a proactive approach by detecting incidents before they can occur. This requires a network of organizations that voluntarily share information about incidents. As a result, an incident in one organization becomes an early warning for others. The second is a national response network. The NCSC closely cooperates with public and private Computer and Emergency Response Teams (CERTs) to create a network that could handle large incidents in the Netherlands. The last mentioned network makes the bundling of expertise and sharing of knowledge possible between all the relevant parties. To achieve this, several Information Sharing and Analysis Centers[4] (ISACs) are established. Every sector dealing with cyber security issues has its own ISAC, a public–private partnership wherein parties involved share information and experiences. The sectors involved are, for example, telecom, water, airport, and financial. Each ISAC has three public institutions involved: the NCSC, the General Intelligence and Security Service of the Netherlands, and Team High Tech Crime of the Dutch National Police. Additionally, every ISAC has sector-dependent representatives. Participants of an ISAC meet periodically, varying from twice a year to eight times a year. An example of the information sharing is the cooperation between the banking industry and the government as a result of several DDoS attacks on the digital payment systems. Since information sharing strongly depends on mutual trust, it is hard to

[4]ISACs are not typically Dutch, but an international phenomenon.

measure cooperation efforts and outcomes (Dunn Cavelty and Suter 2009) which hamper evaluation of such practice.

However, the Dutch approach has its limitations. Lodder and Toet (2013) state, for example, that the division of competences amongst several governmental authorities is problematic with respect to cybersecurity. In case of crime threats, the police is the dedicated actor, in case of terrorism it is the General Intelligence and Security Service of the Netherlands. The NCSC should provide the combination of these forces, but this has not been realized yet. Another limitation is inherent to the Dutch culture, according to Clark et al. (2014). In line with the so-called *polder model,*[5] government tries to encourage private parties to participate in cybersecurity issues rather than force them to do that. This implicates a bottom-up and consensus-driven approach. The authors state that one of its shortcomings is the long time it takes to produce results. Therefore, in times of crises the consensus model has to be set aside, since clear lines of communication and well-defined roles are crucial for clear communication in situations requiring rapid intervention (Clark et al. 2014).

Nevertheless, Van den Heuvel and Klein Baltink (2014) state that the Dutch approach of bringing all these parties together has resulted in an improved understanding of each other's interests and needs. Furthermore, it stimulated defining common objectives and criteria. Some of these common goals are mobilizing relevant parties in the field of cyber security, building of capacity, developing a proactive attitude to reduce crime and potential damages, learning together from incidents to create a better working environment for public–private participation, and increasing cyber security awareness (Van den Heuvel and Klein Baltink 2014).

9.5 Discussion

Considering a PPP strategy in safety requires the consideration of normative values such as legal protection and democratic control (Hoogenboom and Muller 2002). Due to the NPM strategy, government seems to have lost its traditional position regarding the safety domain and private parties seem to have gained influence, regarding the growth of mass private properties (Van Steden 2011). This raises questions about the position governmental authorities must take: a central leading position which stems from the classic perception of the state as absolute ruler? Or is the government 'just' one of the actors involved? Whose responsibility is it to ensure safety in society? Can the assurance of public values be left over to private parties, who are possibly led through economic motives? The criminological debate concerns two main views.

Some scholars (e.g., Shearing and Wood 2003; Stenning 2009) show that considering government as monopolist is no longer valid due to the growing

[5]This refers to a consensus model, which reflects the striving for consensus in Dutch politics and society.

number of non-state actors acting like government. Garland (2001) characterized this changing conception of central authority and its accompanying absolute power as the 'myth of sovereign state'. This is also called the nodal government paradigm. Nodal governance is a form of governance wherein the government is not the central authority within a cooperative, but just one of the actors involved. 'Nodal' refers to the network society we live in and implies strong interdependence between individuals and between groups. Society consists of various nodes, between which people, goods, money, and information flow. These flows are often considered as the vital infrastructures of society, which attracts criminals (Boutellier 2005). In this view, the withdrawal of the state is considered as a positive development because it creates possibilities to anticipate the needs of society, especially controlling, coordinating, and being liable for a safe society (Van Steden 2011).

Conversely, other criminologists are critical of the implications mentioned, because they associate the withdrawal of governmental authorities with a decrease of democratic control, legitimacy, and social equality when it concerns the distribution of safety as public good (Yar 2011). Loader and Walker therefore developed the concept of anchored pluralism, assuming that cooperation between government and private actors can only be established justly within the boundaries of the democratic, rule of law society, i.e., anchored with the democratic foundation in order to guarantee the public interest (Loader and Walker 2007). Core principles which should be taken into account when exercising authority are democratic legitimacy, legal certainty, and the equality before law. These are meant to ensure the protection of fundamental rights of citizens and should be guaranteed, also in situations wherein private parties assist governmental institutions.

Concluding, it is no longer the question whether public and private organizations should cooperate, but how this must be realized. As shown, the division of tasks and responsibilities is a complex question, but worth of thinking of thoroughly. In the end, safety as a public interest is a value to look after, not only offline but also in cyberspace.

9.6 Summary and Conclusions

As shown in this chapter, many actors play a role in the field of digital safety. Since the police face several difficulties, such as a lack of capacity and knowledge of cybercrime, an alternative strategy might be helpful to overcome these. Private parties can contribute by means of sharing information and expertise, coordinated action, and the deployment of people. However, starting a PPP is not a sinecure since the actors involved differ from each other in several ways. The overall conclusion is that the success of cooperation depends on the ability of dealing with the differences and making use of them, instead of letting them hamper cooperation.

References

Bekkers, V., van Sluis, A., & Siep, P. (2006). *De nodale oriëntatie van de Nederlandse Politie: Over criminaliteitsbestrijding in de netwerksamenleving: Bouwstenen voor een beleidstheorie*. [The nodal orientation of the Dutch police: About crime fighting in the network society]. Rotterdam: Erasmus Universiteit Rotterdam.

Boonstra, J. J. (2007). Ondernemen in allianties en netwerken: Een multidisciplinair perspectief. [Undertaking in alliances and networks. A multidisciplinary approach]. *M&O,* 3/4, 5–25.

Bossler, A. M., & Holt, T. J. (2012). Patrol officers' perceived role in responding to cybercrime. *Policing: An International Journal of Police Strategies & Management, 35*(1), 165–181.

Boutellier, H. (2005). *Meer dan veilig. Over bestuur, bescherming en burgerschap*. [More than safe. About governance, protection and citizenship]. Den Haag: Boom Juridische Uitgevers.

Brinkerhoff, D. W., & Brinkerhoff, J. M. (2011). Public-private partnerships: Perspectives on purposes, publicness, and good governance. *Public Administration and Development, 31*, 2–14.

Capeller, W. (2001). Not such a neat net: Some comments on virtual criminality. *Social and Legal Studies, 10*, 229–242.

Clark, K., Stikvoort, D., Stofbergen, E., & van den Heuvel, E. (2014). A Dutch approach to cybersecurity through participation. *IEEE Security and Privacy, 12*, 27–34.

Décary-Hetú, D., & Dupont, B. (2012). The social network of hackers. *Global Crime, 13*(3), 160–175.

Domenie, M. M. L., Leukfeldt, E. R., van Wilsem, J., Jansen, J., & Stol W. P. (2013). *Slachtofferschap van delicten met een digitale component onder burgers. Hacken, malware, persoonlijke en financiële delicten in kaart gebracht.* [Victimization of crimes with a digital component: a report on hacking, malware, personal and financial crimes]. De Bilt/Leeuwarden: PAC/NHL Hogeschool.

Dunn Cavelty, M., & Suter, M. (2009). Public-private partnerships are no silver bullet: An expanded governance model for critical infrastructure protection. *International Journal of Critical Infrastructure Protection,*. doi:10.1016/j.ijcip.2009.08.006.

ENISA (2011). *Cooperative models for effective public private partnerships. Good practice guide*. Retrieved May 29, 2015 from https://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/national-public-private-partnerships-ppps/good-practice-guide-on-cooperatve-models-for-effective-ppps.

Garland, D. (2001). *The culture of control: Crime and social order in contemporary society*. Chicago: The University Press of Chicago.

Gogolin, G., & Jones, J. (2010). Law enforcement's ability to deal with digital crime and the implications for business. *Information Security Journal: A Global Perspective, 19*(3), 109–117.

Grabosky, P. N. (2000). *Computer crime: A criminological overview*. Prepared for presentation at the Workshop on Crimes Related to the Computer Network, Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Vienna, 15 April 2000. Retrieved August 7, 2012 from https://www.ncjrs.gov/App/publications/Abstract.aspx?id=209342.

Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? *Social and Legal Studies, 10*, 251–256.

Hagenaars, P. M. M., & Bonnes, J. M. (2014). *De kracht van privaat-publieke samenwerking [The power of private-public cooperation]*. Den Haag: Boom Juridische Uitgevers.

Heldeweg, M., & Sanders, M. (2011). Botsende waarden bij publiek-private samenwerking. Dimensies en dilemma's van juridisch-bestuurskundige legitimiteit, in het bijzonder bij openbaar gezag [Clashing values in public-private partnerships. Dimensions and dilemmas of judical-governmental legitimacy, especially in public authority]. *Bestuurskunde, 2*, 33–43.

Hodge, G., & Greve, C. (2005). Introduction. In G. Hodge & C. Greve (Eds.). *The challenge of public-private partnerships. Learning from international experience* (pp. 1–21). Cheltenham: Edward Elgar Publishing Limited.

Holt, T. J., & Bossler, A. M. (2012). Police perceptions of computer crimes in two south-eastern cities: An examination from the viewpoint of patrol officers. *American Journal of Criminal Justice, 37*(3), 396–412.

Holt, J. T., & Lampke, E. (2009). Exploring stolen data markets online: Products and market forces. *Criminal Justice Studies, 23*(1), 33–50.

Hoogenboom, A. B., & Muller, E. R. (2002). *Voorbij de dogmatiek. Publiek-private samenwerking in de veiligheidszorg*. [Past dogmatic. Public-private cooperation in safety assurance]. Apeldoorn: Politie & Wetenschap.

Hudson, B., Hardy, Henwood, M., & Wistow, G. (1999). In pursuit of inter-agency collaboration in the public sector. *Public Management: An International Journal of Research and Theory, 1*(2), 235–260.

Hunton, P. (2011). The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation. *Computer Law & Security Review, 27*(1), 61–67.

Jewkes, Y., & Leukfeldt, E. R. (2012). Policing cybercrime. In E. R. Leukfeldt & W. P. Stol (Eds.), *Cyber safety: An introduction* (pp. 253–266). The Hague: Eleven International Publishers.

Jewkes, Y., & Yar, M. (2008). Policing cybercrime in the twenty-first century. In T. Newburn (Ed.), *Handbook of policing* (pp. 280–607). Cullompton, UK: William.

Klijn, E. H., Edelenbos, J., Kort, M., & van Twist, M. (2008). Facing management choices. An analysis of managerial choices in 18 complex environmental public private partnership projects. *International Review of Administrative Science, 74*(2), 251–278.

Klijn, E. H., & van Twist, M. (2007). Publiek-private samenwerking in Nederland. Overzicht van theorie en praktijk. [Public-private partnerships in the Netherlands. Overview of theory and practice]. In J. J. Boonstra, (Ed.). *Ondernemen in allianties en netwerken. Een multidisciplinair perspectief* (pp. 156–170). Deventer: Kluwer.

Koops, E. J. (2010). The internet and its opportunities for cybercrime. In M. Herzog-Evans (Ed.), *Transnational criminology manual* (pp. 735–754). Nijmegen: Wolf Legal Publishers.

Leukfeldt, E. R., Domenie, M., & Stol, W.P. (2010). *Verkenning cybercrime in Nederland 2009*. [Cybercrime in the Netherlands]. Den Haag: Boom Juridische Uitgevers.

Leukfeldt, E. R., Veenstra, S., Domenie, M., & Stol, W. P. (2013a). *De strafrechtketen in een gedigitaliseerde samenleving. Een onderzoek naar de strafrechtelijke afhandeling van cybercrime*. [Criminal justice in a digitized society. A study into the criminal prosecution of cybercrimes]. De Bilt/Leeuwarden: PAC/NHL.

Leukfeldt, E. R., Veenstra, S., & Stol, W. P. (2013b). High volume cyber crime and the organization of the police. The results of two empirical studies in the Netherlands. *International Journal of Cyber Criminology, 7*(1), 1–17.

Loader, I., & Walker, N. (2007). *Civilizing security*. Cambridge University Press.

Lodder, A. R., & Toet, J. (2013). Cybersecurity: Europese Unie initiatieven voor een intrinsiek grensoverschrijdend fenomeen. [Cybersecurity: European Union initiatives for an intrinsic boarder-crossing phenomenon]. *Tijdschrift voor internetrecht,* 5/6, 135–140.

Lu, Y., Luo, X., Polgar, M., & Cao, Y. (2010). Social network analysis of a criminal hacker community. *Journal of Computer Information Systems, 51*(2), 31–41.

NCSC (2014). *Cybersecuritybeeld Nederland. CSBN-4*. Den Haag: Ministerie van Veiligheid en Justitie.

NCSC (s.d.). *ISACs*. Retrieved April 23, 2015 from https://www.ncsc.nl/organisatie/publiek-private-samenwerking/isacs.html.

Onderzoeksraad voor Veiligheid (2012). *Het Diginotarincident. Waarom digitale veiligheid de bestuurstafel te weinig bereikt* [The Digitnotar incident. Why digital safety does reach the management table too little]. Retrieved April 23, 2015 from http://www.onderzoeksraad.nl/uploads/items-docs/1094/Rapport_Diginotar_NL_web_def_20062012.pdf.

Osborne, D., & Gaebler, T. (1992). *Reinventing government. How the entrepreneurial spirit is transforming the public sector*. Boston: Addison-Wesly.

Peretti, K. K. (2008). Data breaches: What the underground world of "carding" reveals. *Santa Clara Computer and High Technology Law Journal, 25*, 345–414.

Rittel, H. W. J., & Webber, M. M. (1973). Dilemmas in a general theory of planning. *Policy Sciences, 4*, 155–169.

Schuilenburg, M. (2012). *Orde in veiligheid. Een dynamisch perspectief.* [Orderliness in safety. A dynamic perspective]. Den Haag: Boom Lemma Uitgevers.

Shearing, C., & Wood, J. (2003). Nodal governance, democracy, and the new 'denizens'. *Journal of Law and Society, 30*(3), 400–419.

Smit, M. (2010). *Publiek belang: hoe houd je het op de rails. Een studie naar de effectiviteit van planvorming voor stationslocaties*. [Public interest: how to keep it on track. A study into the effectiveness of planning of railway-station locations]. Enschedé: Gildeprint.

Soudijn, M. R. J., & Monsma, E. (2012). Virtuele ontmoetingsruimten voor cybercriminelen. [Virtual meeting places for cyber criminals]. *Tijdschrift voor Criminologie, 54*(4), 349–360.

Soudijn, M. R. J., & Zegers, B. C. H. T. (2012). Cybercrime and virtual offender convergence settings. *Trends in Organized Crime, 15*, 111–129.

Stenning, P. (2009). Governance and accountability in a plural policing environment. The story so far. *Policing, 3*(1), 22–33.

Stol, W. P., Kaspersen, H. W. K., Kerstens, J., Leukfeldt, E. R., & Lodder, A. R. (2008). *Filteren van kinderporno op internet. Een verkenning van technieken en reguleringen in binnen- en buitenland.* [Filtering of child pornography on the internet. Technologies and laws in the Netherlands and abroad]. Den Haag: Boom Juridische Uitgevers.

Stol, W. P., Kaspersen, H. W. K., Kerstens, J., Leukfeldt, E. R., & Lodder, A. R. (2009). Governmental filtering of websites: the Dutch case. *Computer Law & Security Review, 25*(3), 251–262.

Stol, W. P., Leukfeldt, E. R., & Klap, H. (2013). Policing a digitized society. The state of affairs in the Netherlands in 2013. In W.P. Stol & J. Jansen (Eds.), *Cybercrime and the Police* (pp. 61–74). Eleven International Publishing: The Hague.

Struiksma, N., de Vey Mestdagh, C. N. J., & Winter, H. B. (2012). *De organisatie van de opsporing van cybercrime door de Nederlandse politie.* [The organization of policing cybercrime in the Netherlands] Apeldoorn: Politie & Wetenschap.

Terpstra, J. (2011). Regulering in een hybride veiligheidszorg. Over de bewaking van een publiek goed in een deels geprivatiseerd bestel [Regulation in hybrid safety assurance]. *Tijdschrift voor Veiligheid, 10*(4), 41–58.

Terpstra, J., & Kouwenhoven, R. (2004). *Samenwerking en netwerken in de lokale veiligheidszorg.* [Cooperation and networks in local safety assurance]. Kerckebosch: Zeist.

Toutenhoofd-Visser, M. H., Veenstra, S. Domenie, M. M. L., Leukfeldt, E. R., & Stol, W. P. (2009). *Politie en cybercrime. Intake en eerste opvolging. Een onderzoek naar de intake van het werkaanbod cybercrime door de politie.* [Police and cybercrime. A study on the registration process with regard to cybercrime reports within the Dutch police]. Leeuwarden: NHL Hogeschool.

Van Delden, P. (2009). *Samenwerking in de publieke dienstverlening. Ontwikkelingsverloop en resultaten*. [Cooperation in public services. Development and outcomes]. Delft: Eburon.

Van den Heuvel, E., & Baltink, G. K. (2014). Coordination and cooperation in cyber network defense: the Dutch efforts to prevent and respond. In M. Hathaway (Ed.) *Computer Network Defense: Incident Detection and Response* (pp. 118–129). NATO Science for Peace and Security Series.

Van der Hulst, R. C. & Neve, R. J. M. (2008). *High-tech crime: Inventarisatie van literatuur over soorten criminaliteit en hun daders.* [High tech crime. Literature review of cybercrimes and their offenders]. Den Haag: WODC.

Van Montfort, C. J. (2008). *Besturen van het onbekende. Goed bestuur bij publiek-private arrangementen.* [Governing the unknown. Good governance in public-private arrangements]. Den Haag: Boom Lemma Uitgevers.

Van Montfort, C., van den Brink, G., Schulz, M., & Maalsté, N. (2012). *Publiek-private samenwerking in maatschappelijke veiligheid*. [Public-private partnerships in social safety]. Den Haag: WODC.

Van Steden, R. (2011). Sturing van lokale veiligheid: een achtergrondstudie. [Governance of local safety: a background study]. In R. van Steden (Ed.). *Strategieën van lokale veiligheid. Een achtergrondstudie en drie reflecties* [Strategies of local safety. A background study and three reflections] (pp. 9–51). Amsterdam: Amsterdam University Press.

Veenstra, S., Zuurveen, R., Jansen, J., Kloppenburg, S., & Stol, W. P. (2014). *MKB en cybercrime. Slachtofferschap onder het Nederlandse Midden- en Kleinbedrijf in een gedigitaliseerde samenleving.* [SMEs and cybercrime. Victimization of the Dutch Small and Medium-sized Enterprises in a digitized society]. Leeuwarden/Apeldoorn/Heerlen: NHL Hogeschool/ Politieacademie/Open Universiteit.

Visser, R. A., van Gemerden, E., More, P. A., & de Roon, R. J. C. (2008). *Sturing en samenwerking in handhavingsprojecten. [Governance and cooperation in enforcement projects]*. Leiden: Leiden University Press.

Wall, D. S. (1997). Policing the virtual community: The internet, cyber crimes and the policing of cyberspace. In P. Francis, P. Davies & V. Jupp (Eds.) *Policing futures, the police, law enforcement and the twenty-first century* (pp. 208–236). London: Macmillan.

Wall, D. S. (2007/10). Policing cybercrimes: Situating the public police in networks of security within cyberspace (Revised May 2010). *Police Practice & Research: An International Journal, 8*(2), 183–205.

Yar, M. (2011). From the 'governance of security' to 'governance failure': refining the criminological agenda. *Internet Journal of Criminology*. Retrieved April 23, 2015 from http://www.academia.edu/2803630/from_the_governance_of_security_to_governance_failure_refining_the_criminological_agenda.

Yip, M., Shadbolt, N., & Webber, C. (2012). *Structural analysis of online criminal social networks. ISI 2012.* June 11–14, 2012, Washington.

Zhang, L., Young, R., & Prybutok, V. (2007). Inhibitors of two illegal behaviors: Hacking and shoplifting. *Journal of Organizational and End User Computing, 19*(3), 24–42.

Chapter 10
Cyber Security Challenges: The Israeli Water Sector Example

Lior Tabansky

Abstract Critical infrastructure protection spans an increasing number of publicly and privately owned nondefense entities. As cyberspace continued to expand, securing society requires a comprehensive approach to include business sector cooperation with all levels of government. More attention must be devoted to activities and facilities not only on the national but also on the municipal level. This will require nontraditional governance approaches to complement the usual top–down national regulation. We discuss recent cyber security policy developments in Israel, and move on to discuss future cyber security challenges using water supply as an example. Hopefully the approaches discussed in this paper will provide useful information for other developed countries.

Acronyms

BOT	Build–operate–transfer
BYOD	Bring your own device
CIP	Critical infrastructure protection
CoTS	Commercial off-the-shelf
DDR&D	(*Maf'at* מפא"ת) Ministry of Defense Directorate for Research & Development
DOD	Department of Defense
ICS	Industrial control system
IDF (*Tzahal* צה"ל)	Israel Defence Forces
ILITA	Information and Technology Authority
INCB	Israel National Cyber Bureau
ISA (*Shabak* שב"כ)	Israel Security Agency
IT	Information technology

L. Tabansky (✉)
The Blavatnik Interdisciplinary Cyber Research Center (ICRC)
and the Department of Political Science, Tel Aviv University, 39040,
6997801 Tel Aviv, Israel
e-mail: cyber.ac.il@gmail.com

R.M. Clark and S. Hakim (eds.), *Cyber-Physical Security*,
Protecting Critical Infrastructure 3, DOI 10.1007/978-3-319-32824-9_10

Kinneret	Lake of Galilee
Maf'at	The Ministry Of Defense Directorate For Defense Research And Development
Mekorot	National Water Company
MCM	Million cubic meters
NCI	National Cyber Initiative
NCSA	(*Rashut Le'umit le-Haganat ha-Cyber* רשות לאומית להגנת הסייבר) National Cyber Security Authority
NISA	(*Re'em*) National Information Security Authority
NSA	National Security Agency
PLC	Programmable logic controller
SCADA	Supervisory control and data acquisition
Shodan	Web Search Engine for Finding Interconnected Devices
USB	Universal Serial Bus
WWW	World Wide Web

10.1 Introduction

Israel perceives cyber security as intrinsically integrated with physical security. To mitigate cyber-physical risk, a centralized civilian Critical infrastructure protection regulation was enacted in Israel in 2002. As will be discussed, in recent years, the Israeli cyber security policy refocuses on the civilian sector at large. The Israeli experience demonstrates that comprehensive cyber-physical security depends on the political ability to reach acceptable trade offs between often competing values and various stakeholders throughout the public and business sector, as much as Information Technical (IT) security capacity.

We also discuss the water sector in Israel and the common cyber security risks and controls to illustrate future cyber security challenges. Water infrastructure is universally considered critical. The fresh water supply sector in Israel is an interconnected network of advanced computerized process technologies, and a similarly complex web of stakeholders, owners, suppliers, operators, and contractors. However, the cyber security policy almost exclusively addresses the national level.

Finally, we will discuss the need to include the municipal level and small–medium business in the cooperative cyber security effort. The answer to future cyber security challenges should include a greater integration of both the private and public sector, and of local and national governments rather than applying a top-down centralized approach. Perhaps the use of public–private partnerships would provide a useful model for solving future cyber security problems at the local and national level.

10.2 Cyber-Physical Security at the State Level: What Role for a Government in Critical Infrastructure Protection?

The American defense sector has been the global driver of microelectronics, networking and other cyber technology building blocks (Mazzucato 2013). The understanding of the subject matter was accumulated in the defense sector after years of experience. The first outcome of this understanding is the recognition that there is a new risk. The next step was to communicate the change, for the state has an interest in reducing the risk. Eventually, once the government decides to share some responsibility in critical infrastructure protection (CIP), the issue becomes practical: navigating and designing an effective response throughout the range of policy making and policy implementation options.

10.2.1 Critical Infrastructure Protection in Israel

The Israeli defense sector has been traditionally willing to invest in research and development to achieve qualitative advantage over its neighbors. Therefore, in Israel, many other developed states, defense and military agencies were the early developers and users of cyber technology. During the late 1990, *Maf'at* (the Ministry of Defense Directorate for Defense Research & Development) has been communicating concerns about cyber vulnerabilities of Israeli civilian infrastructure, to the other government branches on the national level. The concerns stemmed from the early experience with technological change *Maf'at* has accumulated, and the insight that the risks are not limited to the military environment. Communicating these concerns outside the defense establishment was the initiative of *Maf'at* leadership rather than the directorate's designated duty.

Confronting a national cyber security risk via the free will of profit-driven market forces—was rejected almost instantaneously in Israel. The role of misaligned market incentives in cyber insecurity was only later emphasized by economists who established the subfield "Economics of Information Security" (Anderson and Moore 2006).

Increased government involvement in market activities for the public good of cyber-physical security was accepted in Israel since 2002. While even today the Internet and the World Wide Web (WWW) are too often conflated with cyberspace, 'Cyberspace' was not viewed as a virtual environment of information. On December 11, 2002 Government of Israel Special Resolution B/84 on 'The responsibility for protecting computerized systems in the State of Israel was one of the first active CIP policies in the developed world. It defines the responsibility for protecting computer-integrated control and supervision systems, which controls and supervises measureable activities carried out by mechanized means within the information system itself. The Israeli utilities providers such as water, energy, and transport were designated critical from the start. Financial services and telecom

providers were increasingly deemed critical in the modern economy, and eventually the CIP regulation was expanded to include most of these sectors as well.

The Israeli CIP approach prioritized cyber-physical security: computerized information systems are seen as interconnected with physical realms. The resolution focuses entirely on the civilian cyber-physical security activities. The law defines 'activities for protecting critical computerized systems' as 'activities required to preserve critical computerized systems, information stored in them, confidential information related to them, as well as preventing damages to those systems or the information in question'.

The Israeli Defense Forces (IDF) was then leaders in Information Technology (IT) security matters. However, designating the responsibility for protecting vital computerized systems of civilian publicly- and privately owned bodies to the military creates an immense ethical and legal problem in Israel's democratic society. The military has no legal authority for domestic operation, and the military-centric approach for national cyber-physical security was rejected.

On the other hand, an establishment of a new dedicated agency for cyber security at large, or for CIP specifically, required prolonged democratic legislative and administrative processes to overcome existing statutory issues.

The Israeli law permits only *Shabak* [Israel Security Agency (ISA)] and the police to intervene in civilian matters for specific security purposes. The Police and ISA operate under a comprehensive legal framework and strict judicial supervision. During early 2000s, the Israeli security services were overwhelmed by the Palestinian 'suicide bombers intifada',[1] on top of common crime fighting duties. In fact, most of the public Israeli attention was then devoted to homeland security efforts. This context demonstrates that any policy is a result of a set of political and external constraints.

10.2.2 The National Information Security Authority (Re'em)

The National Information Security Authority was established in *The Shabak* by the 2002 resolution as 'the national unit for the protection of vital computerized systems'. *Shabak's* Protective Security Division was already in charge of government's information security concerns. It also enjoyed the appropriate legal foundation in the 'Regulation of Security in Public Bodies Law of 1998' and the *Shabak* Statute. The 1998 law was amended to provide the new regulators the authority to supervise public bodies—organization that operates infrastructure designated critical. Despite the word 'public', private ownership of 'critical infrastructure' the law covers both in the *public* not-for-profit and the *private for-profit* sectors.

[1]Israelis were targeted by terrorists on the streets, cafes, and buses in a cycle of violence that claimed the lives of 319 Israeli soldiers and 745 civilians, and left 2430 soldiers and 5032 civilians wounded.

Re'em auditors may access any relevant information and assets of the organization to ensure compliance with their instructions and to assess existing and new risk vectors. The supervised organization continues to finance all operations, protection, maintenance, upgrading, backup, and recovery of its critical IT systems, including the changes, enhancements, and equipment mandated by *Re'em*, and to share information and activities with the regulator. The requirements were identical for both privately owned businesses and state-owned utilities. While some interpretations of the Israeli 'Regulation of Security in Public Bodies Law of 1998' law state that officials may be held liable for neglecting to comply with the Law's demands—criminal sanctions were not yet tested in real legal scenario.

By 2012, *Re'em* regulated cyber security aspects in 27 critical national infrastructure bodies, including the Israel Electric Corporation, the *Mekorot* Water Company, and Israel Railways.

10.3 Cyber security of the Israeli Fresh Water Supply System

The Israeli arrangement was advanced, but not perfect. To demonstrate the need to include the municipal and small–medium business levels in the cooperative cyber security effort, we discuss the Israeli fresh water supply system. Most of the Middle East approaches—or already suffers from—physical scarcity of water resources. As will be discussed Israel is addressing this problem through the application of desalination technology. Moreover, strategic forecasts describe the deterioration of water scarcity due to population increase, urbanization, developments, and climate changes. Security planners worldwide increasingly describe scenarios when water shortages escalate into communal violence and international armed conflict. Water-related conflicts are common in the region and water issues form a central part of regional agreements. Israel has seen its share of water-related conflicts with Syria and Lebanon, and has reached lasting arrangements with the Kingdom of Jordan on riparian right to water in the Jordan River basin.

Israel has always been investing heavily in improving water availability and quality to all its citizens, for consumption, agriculture, and industry. Israeli drip irrigation technology and crop modification provide prominent examples on the role of science and technology in reducing the demand for water. On the supply side, common examples are the Israel National Water Carrier completed in June 1964 to transport water from Lake of Galilee (*Kinneret*) to the coastal *Sharon* Plain and eventually to the *Negev* desert; reclamation of wastewater; rain water harvesting and increasing the operational efficiency of water distribution networks. Concerns about water shortages or scarcity, climate change, and environmental protection have pushed forward further reforms, most importantly sea water desalination (Fig. 10.1).

Fig. 10.1 Israel National Water System Map, The Water Authority (2014)

The Israeli water system is highly integrated and has undergone substantial development to address the challenge of natural resource overuse.[2] Since the late 1990s, Israel has constructed large-scale desalination plants located along the Mediterranean coast and in Eilat (on the Red Sea coast). In 2014, they provided 600 million cubic meters (MCM) a year and are expected to reach 750 MCM/year capacity by 2020. Seawater and brackish water are expected to provide a third of total water demand in Israel by 2020 (OECD 2015). These plants were built as build–operate–transfer (BOT) model: a private for-profit company receives a concession from the public sector to finance, construct, and operate a facility and to recover its expenses in the defined period by collecting revenue. Recycling has also been rapidly developing: 3/4 of the wastewater is being treated to secondary and tertiary levels and later used for agriculture, industry, gardening, etc., to spare expensive drinking water.

Ground and surface water are publicly owned. Government ministries and the Water Authority plan and manage the water system on a national level. The national water company (*Mekorot*) is owned by the government and supplies 70 % of all consumed water in the country. In the context of this research, *Mekorot* has been deemed critical infrastructure and regulated by *Re'em* since the start. Mekorot's water supply system unites most regional water plants, the National Water Carrier System and the Yarkon Negev Facility. Mekorot integrates water from the Lake of Galilee (Kinneret), the coastal and mountain aquifers, drilling waters, sea water and desalinated waters.

However, local infrastructure for delivery of water to consumers, charging for consumption by volume, quality monitoring and sewage treatment are provided on the municipal level. Regional and municipal Water Corporations purchase their entitlements from the central water company (*Mekorot*) and are legally responsible for their delivery to end users. Private subcontractors rather than the municipalities increasingly perform the majority of infrastructure work.

This incomplete schematic description of the sector is sufficient to demonstrate an organizational complexity. In this case, a centralized top–down policy in the sector will necessarily leave numerous loopholes. While it is the correct approach to focus on the larger elements first, and thus provide regulatory cyber-physical security guidance to *Mekorot*, many other risks remain unmitigated.

10.3.1 Threat Assessment: Technology

Modern water systems are comprised of sources, treatment, distribution, and reclamation. Each stage generally has multiple subsystems and components of varying complexity—such as water mains, pumps, hydraulics, valves, hydrants,

[2]The Stephen and Nancy Grand Water Research Institute at the Technion and its founder Prof. Uri Shamir are the focal point of water related research and policy in Israel.

service lines, and storage facilities. Supervisory Control and Data Acquisition (SCADA) systems continuously monitor infrastructure, system condition, and water quality at strategic locations in the system, both in real time and on a periodic basis. Data from these monitoring stations is automatically transmitted over computer networks to a central information management system, and then analyzed to detect abnormal conditions. The central change is the increased computerization and interconnection of industrial control system (ICS), and SCADA which are indispensable in any large-scale industrial activity today.

This technological progress introduces new opportunities and risks (Weiss 2014). We briefly reintroduce the common IT security terms to facilitate the discussion. IT presents new risks, such as those stemming from hardware or software failure. IT security controls are specific activities to address and mitigate IT risks. Risk management refers to a coordinated set of activities and methods that is used to control the risks that can affect it.

The term 'attack surface' describes all of the different points where an attacker could get unauthorized access into an information system, and where an attacker could get data out of the system. Each of such points is called an 'attack vector'. Examples include: physical access to serial or Universal Serial Bus (USB) connection, logical access to the system, and additional infrastructure over various networking protocols. Attack vector often is created by exploiting vulnerability. Vulnerability is something in the actual behavior of the system that deviates from the intended behavior, and is very common in software.

Digital controllers and digital communication networks have increasingly been present in industrial systems for several decades. Communication technologies undergo standardization and commodification leading to the proliferation of similar or identical hardware and protocols in SCADA systems. Devices with wireless communication are preferred for operating in remote locations, given their reduced installation cost compared to wired solutions. Today, wireless devices became an integral component of civilian SCADA solutions for components of spatially distributed systems. As wireless communications naturally have a broader attack surface than wired links, many potentially critical facilities are now accessible even via the WWW (Bodenheim et al. 2014). Therefore, if the risks are not mitigated by controls, the attack surface of all industrial processes continues to rapidly expand.

In addition to experimental works, several real-world cyber-attacks affecting SCADA systems, which clearly illustrate critical infrastructure vulnerabilities, were documented. In 2000, an Australian man hacked into the Maroochy Shire, Queensland waste management system, and repeatedly caused millions of liters of raw sewage to spill out into local parks and rivers. The man was a disgruntled ex-employee of contractor that supplied control system technology, and thus had close knowledge of the SCADA system and the wireless access possibility.

Stuxnet, the malware specifically written to infiltrate and silently disrupt industrial control systems (Singer and Friedman 2014; Farwell and Rohozinski 2011), was by far the most harmful cyber-physical attack recorded to date. The malware, discovered in 2010, slowly damaged the centrifuges at Natanz nuclear enrichment facilities in Iran by reprogramming the Siemens-made programmable

logic controller (PLC) that controlled the IR-1 centrifuges to spin the motor out of the safe range (Langner 2011). To do that, it had to first compromise a Microsoft Windows system, and then propagate stealthily inside corporate air-gapped networks. The malware probably had been implanted in late 2007; by the end of 2010, the worm had infected approximately 100,000 hosts in dozens of countries, 60 % of which were in Iran (Sanger 2012). However, it only executed the payload when it found that the target matched the specific configuration. Importantly, Stuxnet took over the human–machine interface (HMI) output to display activity as normal and suppress alarms to evade detection (Katz and Hendel 2012). Before Stuxnet started sabotaging ongoing processes, it intercepted input values from sensors—for example, the state of a valve or operating temperatures—recorded these data, and then provided the legitimate controller code with pre-recorded input signals, while the actual processes in the background were manipulated (Langner 2011). Stuxnet broke the traditional Network Segmentation and perimeter defense paradigms—although these linger on in most InfoSec communities. This was a very complicated and advanced operation.

10.3.2 Threat Assessment: Organization

It is safe to assume that local water subsystems are generally less protected than the Iranian nuclear enrichment plant. Therefore, several vulnerabilities are likely to be present any time in local water subsystems. These can be successfully exploited even by average adversaries, not only to access the local segments but to propagate throughout the national system. The main reason for this is that ICS network architecture is generally flat: the network router multicasts the addresses of all the devices within the entire network's domain, so data can be sent and received from those devices. Once any part of a flat network is breached, the intruder can access the whole domain. Considering the modern wireless instruments increasingly implemented in subsets of municipal level water systems, the adversary has a very substantial attack surface for reconnaissance, persistent hardware breach, malware delivery, and digital payload execution. Since water is a vital service, it should be assumed that adversaries with sufficient cyber capabilities would not hesitate targeting the water system.

10.3.3 Hardware Supply Chain: Attack Scenario A

The defense sector is famous for rigorous operational security procedures, including screening and validating the quality of suppliers and equipment it purchases (Reed et al. 2014). One should assume that for critical infrastructure as well a similar procedure exists, and yet even the US Department of Defense (DoD) has been found to use counterfeit electronic devices (Gorman 2012).

When assessing the supply chain of water subsystems on the municipal level, it is clear that the awareness of the risk and the relevant measures are almost nonexistent. This means that the local water subsystems contain plenty commercial off-the-shelf (CoTS) devices and components, procured from the lowest bidder, and consequently installed with the default security settings. One does not have to be an intelligence officer to know this. The situation is now evident from the comfort of your home: just run a search on Shodan—the Web search engine for finding Internet-connected devices. Hundreds of thousands of unexpected devices are connected to, and accessible from, the Internet and the WWW (Bodenheim et al. 2014).

For a dedicated attacker, the lower level of security awareness and controls on a municipal level provides a good opportunity to install hardware Trojan horses. While malware is dependent on software configuration, hardware enables stealthy persistent unlimited access to the water system. An "infection" introduced at one point at the municipal level could easily spread to the entire system.

10.3.4 Contractor as a Trusted Insider: Attack Scenario B

Trusted insiders' theft, espionage, and sabotage involving computer networks can cause the most serious damage, most recently manifested by Edward Snowden. Snowden was employed by a contractor of the National Security Agency (NSA)—likely the most competent cyber security organization in the world. Dealing with insider threat is not new to intelligence agencies or financial sector institutions. Common mitigations include systematic personnel management and IT security systems to monitor activity of privileged accounts. Both of these mitigation techniques should be routinely practiced at the local and municipal level.

Contractors should be considered major attack vector even more than directly employed personnel. First, they have the necessary access privileges, but are not under the human resource management of the relevant authority. Second, even if the contractor personnel have no malicious intent, the skilled attacker can target their devices, such as a laptop. As the bring-your-own-device (BYOD) model prevailed, the contractor's consumer grade laptop and smartphone present a good opportunity to breach the ICS system. This attack vector exists even if the personnel are benevolent. At minimum, such approach provides for initial reconnaissance. Once the breach vector is established, the attacker has the time and the liberty to proceed. Contractor personnel should receive the same screening as do the water system employees.

10.4 The Limits of National CIP

Since the late 1990s, the dominant economic ideology in Israel was liberal: the belief that government intervention stifles the innovation and productivity of the free market. This ideology remains one of the prominent opponents to further

complicating the already cluttered Israeli regulatory environment. The difficulty in relinquishing a core duty of the state to the market's "invisible hand" was present despite the predominantly neoliberal economic ideology of the Israeli elite. But in other matters of safety and security, similar government intervention in a liberal economy has been acceptable, in Israel as well as in other capitalist democracies. Residential and office permits require sanitation and fire measures; driving a motor vehicle requires periodical technical inspection, a driving license and mandatory insurance; building standards define the methods and materials to be used to withstand the forces of nature. With regard to public health, the food and medication industries and markets are heavily regulated. From prescription to nonprescription drugs, cosmetics, dietary supplements, livestock feeds, raw, and prepared foods to drinking water—methods of regulation and enforcement have almost universally become consensual. All such measures interfere with the economic rational to maximize profit, and were usually introduced only after the occurrence of preventable tragedies. During the Twentieth century, such government intervention has led to increased safety, health, and welfare of the average citizen, albeit at the expense of opportunistic profiting by individuals. This rationale should include cyber-physical security. However, debates on the proper delineation of duties between central and local government, industry, and the citizen rage on worldwide.

We describe the path to devise the optimal cyber security policy in Israel, commencing with a central CIP arrangement and evolving into a comprehensive national effort to include the whole civilian sector. As breaches, malfunctions, corporate espionage, and politically motivated leaks were growing in volume and impact, cyber security rose in importance in Israel. In 2010, the Prime Minister established an external independent policy review taskforce on cyber security. The National Cyber Initiative (NCI) was launched in 2010 with the vision to preserve Israel's standing in the world as a center for information technology development, to provide it with superpower capabilities in cyberspace, and to ensure its financial and national resilience as a democratic, knowledge-based, and open society. The main practical recommendation was to establish the Israel National Cyber Bureau (INCB) in the prime minister's office, to promote national capability in cyberspace and to improve Israel's preparedness in dealing with the challenges in cyberspace. It is charged with improving cyber security while advancing Israel's position as a center of cyber technology development by encouraging cooperation between academia, industry and the private sector, government offices, and the defense community.

The INCB has been working on a new, comprehensive national cyber strategy for Israel. In September 2014, *Haaretz* daily newspaper published that staff work on cyber security strategy and authority had deteriorated into a turf battle between *Shabak* and INCB (Ravid 2014). *Shabak* opines that given the professional success of the 2002 CIP arrangement, it is obvious that the optimal cyber security policy is to further expand *Re'em* authority. However, as national cyber security requires a broader range of policy instruments finely tuned to approach various 'customers', the idea of scaling up the CIP arrangement incurred significant controversy. Such

cyber security policy would require a dramatic increase in the mandatory intelligence *Shabak* needed to collect throughout the civilian cyberspace to carry out its operations. The clash of security and privacy values was reignited.

The INCB has thus pushed forward the establishment of a civilian agency to address civilian sector cyber security as part of its mandate to develop strategy and policy. The central argument was that, removing the clandestine intelligence agency from the civilian cyber security front in favor of a civilian organization would mitigate the conflict of values. The opposing arguments revolved around the time it would take to establish an additional organization to provide cyber security, the risks that it will not be effective and efficient, and the fact that a similar function has been performed successfully by *Re'em* for over a decade.

As the designated agencies were gridlocked and could not reach a decision, a new round of governmental and external expert reviews was required to present the government with a feasible solution to the cyber security arrangement.

10.4.1 The National Cyber Security Authority

To achieve the strategic goal of cyber security, a feasible solution to the conflicting values was required. Having steered the 2010 NCI, Professor Isaac Ben-Israel again was tasked by Prime Minister Netanyahu with producing a roadmap towards solving the cyber security policy gridlock. His taskforce consisted of representatives from *Shabak*, INCB, IDF Intelligence Corps SigInt unit, Mossad, National Security Council, Israeli Law, Information and Technology Authority (ILITA) in the Ministry of Justice, the Ministry of Strategic Affairs, and other stakeholders. The Israeli Law, ILITA, the personal data protection unit established in the Ministry of Justice in 2006, is one of the key stakeholders in cyber security policy.[3]

Accepting the recommendation of this 2014 taskforce, the government decided in Resolution 2443 to establish a new agency to enhance cyber security in the civilian sector (Prime Minister's Office 2015). This new National Cyber Security Authority (*Rashut Le'umit le-Haganat ha-Cyber*) will constitute an operative agency to act alongside the INCB, which continues to build and maintain the State of Israel's national strength as an international leader in the field.

As NCSA must better integrate the various capabilities into the national effort, it must receive the necessary legal authority to defend the civilian sphere from cyber threats while keeping the basic freedoms, civil rights and privacy. The NCSA consists of mostly new elements. The public Israel National Cyber Event Readiness Team (CERT-IL)[4] is Israel's national focal point for cyber security incident

[3]ILITA consists of three regulators: the database register, responsible for oversight and enforcement of data protection guidelines; the electronic signature register, and credit score service providers register.

[4]https://cert.gov.il/.

management and handling in order to enhance the national resilience against cyber threats. It provides a single point of contact in Israel regarding cyber security threats and incidents for international corporations, cyber security companies and other Computer emergency response teams (CERTs). The NCSA acknowledges the need to cooperate with existing regulators, operators, and stakeholders in the comprehensive cyber security effort. This is in contrast with the traditional top-down government public policy approach, which tends to legislate, enact, and enforce—with various success levels.

In addition, the subsequent February 15, 2015 Government Resolution 2444 outlines that concentrated regulation, standardization, licensing, auditing, training, instruction, public relations, and international cooperation efforts will be developed. The interfaces between the national capabilities and the local and municipal levels may be enhanced by such standardization, licensing, and auditing. In the water sector, the municipal level may be required to adopt stricter standards regarding operation procedures and cyber security in a feasible scenario. The personnel who provide IT security and operational security relevant functions might be required to undergo cyber security training and licensing. The least feasible scenario would be to use the increased cyber-physical security risk to call for the centralization of water supply functions at the national, instead of the local, level.

The recent policy change allows for enhanced dialog and collaboration between local and municipal stakeholders and the national security officials, towards enhanced cyber security.

10.5 Conclusions: Towards Cyber security on Municipal Level

Since the late 1990s, cyber security issues in Israel were attuned to cyber-physical security. The 2002 CIP arrangement was a very significant and timely step. It has proven to improve cyber-physical security and contribute to national security, resilience, and welfare. In cyber defense, Israel outranked all the major cyber powers, including the US, Russia, and China, according to a 2012 study (Grauman 2012). However, as cyberspace continued its rapid expansion, the policy that is confined to the large entities in designated sectors was becoming increasingly inadequate for Israel. We presented an example: the developing risks to the water sector are present on the local and municipal level, which the existing CIP regulation does not cover.

The protection of the civilian sector at large is the focus of Israeli cyber security policy in the second decade of the twenty-first century. This represents a marked shift from the original cyber security focus on the governmental and military systems and later the civilian critical infrastructure.

This expansion of cyber security to the civilian sector at large presents enormous conceptual and ethical challenges to all modern democratic societies. The security

needs that IT professionals and defense officials advocate often come in tension with the basic freedoms that any democratic society cherishes. The need to balance between competing values is central in national policy, including cyber security. Such acts of balancing require compromise to design acceptable trade offs between the need to manage new risks and the need to preserve the core values of a society. This is the essence of politics rather than of security engineering.

We presented the policy making process leading to the recently achieved Israeli roadmap to mitigate these tensions for comprehensive national cyber security. In 2014, Israeli leadership has overcome a hurdle, common to democracies towards promoting comprehensive nationwide cyber security policy. The NCSA design enhances comprehensive national cyber security while reducing the tension between security needs and basic freedoms. The process of setting up the NCSA includes multiple legislative, organizational, and other efforts aimed to last several years. Whether this approach will successfully integrate the national-level capabilities with local and municipal level structures to improve cyber-physical security, while maintaining the basic freedoms and democratic values—remains to be seen. Interdisciplinary technical, political, and organizational attempts to enhance comprehensive cyber security must continue.

We have used water supply to illustrate the need to develop an integrated national cyber security policy dedicated to protecting critical infrastructure. However, water supply is only one example and it is clear that this approach should be applied to all levels of Israel's society and indeed to all of the developed countries in the world.

References

Anderson, R., & Moore, T. (2006). The Economics of information security. *Science, 314*, 610–613.

Bodenheim, R., Butts, J., Dunlap, S., & Mullins, B. (2014). Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices. *International Journal of Critical Infrastructure Protection, 7*, 114–123.

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival, 53*, 23–40.

Gorman, C. (2012). Counterfeit chips on the rise. *IEEE Spectrum, 49*, 16–17.

Grauman, B. (2012). Cyber-security: *The vexed question of global rules: An independent report on cyber-preparedness around the world*. In (SDA), S. D. A. & INC., M. (eds.). Brussels: Security & Defence Agenda (SDA).

Katz, Y., & Hendel, Y. (2012). *Israel vs. Iran: The shadow war*. Washington, D.C, Potomac.

Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security and Privacy, 9*, 49–51.

Mazzucato, M. (2013). *The entrepreneurial state: Debunking public vs. private sector myths*.

OECD. (2015). *Water resources allocation: Sharing risks and opportunities*. OECD Publishing.

Prime Minister's Office, I. (2015). *Cabinet approves establishment of national cyber authority* (Online). Available: http://www.pmo.gov.il/English/MediaCenter/Spokesman/Pages/spokeCyber150215.aspx.

Ravid, B. (2014). *Israeli security agencies in turf battle over cyber war*. Netanyahu to decide. *HaAretz*, 14/09.

Reed, M., Miller, J. F., & Popick, P. (2014). Supply chain attack patterns: Framework and Catalog. *Office of the Deputy Assistant Secretary of Defense for Systems Engineering*.

Sanger, D. E. (2012). *Confront and conceal: Obama's secret wars and surprising use of American power*. New York: Crown.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford, New York: Oxford University Press.

Israel National Water System Map, The Water Authority (2014).http://www.water.gov.il/Hebrew/ProfessionalInfoAndData/2012/israel_national_water_system-map.pdf

Weiss, J. (2014). Industrial control system (ICS) cyber security for water and wastewater systems. *Securing Water and Wastewater Systems.* Berlin: Springer.

Chapter 11
Efforts to Get People Involved in Cyber-Physical Security: Case Studies of Australia and Singapore

Hee Jhee Jiow

Abstract As critical infrastructures, such as transportation, water, electricity, and gas distribution networks, mature into cyber-physical (CP) systems, they have become more vulnerable to cyber attacks. These attacks have become more sophisticated in nature, and as such, CP security has had to adopt a multi-pronged approach in dealing with it. While technological advancements have been hailed as the main source of safeguard for CP systems, little is mentioned about other contributing factors to CP security, especially if one considers the proliferation of CP systems into more publicly accessible applications such as banking and assisted living. This chapter will examine the efforts to get society involved in CP security specifically in two areas—educational efforts and initiatives to cultivate safe online practices. As Australia and Singapore are developed nations in the usage of CP systems, this chapter will discuss the initiatives undertaken in these two countries.

Abbreviations and Acronyms

ACSC	Australian Cyber Security Centre
AUD	Australian Dollars
BYOD	Bring-Your-Own-Device
CP	Cyber-Physical
FAA	Federal Aviation Administration
NCSM2018	National Cyber Security Masterplan 2018
NUS	National University of Singapore
PIN	Personal Identification Number
SMS	Short Message Service
2FA	2-Factor Authentication

H.J. Jiow (✉)
Singapore Institute of Technology, 10 Dover Drive, Singapore 138683, Singapore
e-mail: jhee.jiow@singaporetech.edu.sg

R.M. Clark and S. Hakim (eds.), *Cyber-Physical Security*,
Protecting Critical Infrastructure 3, DOI 10.1007/978-3-319-32824-9_11

11.1 Introduction

Critical infrastructure, such as transportation networks, electricity generation distribution networks, sophisticated communication systems, water and gas distribution networks, has increasingly relied on the Internet and networked connections for its operations (Pasqualetti et al. 2013). As such, it is frequently referred to as a cyber-physical (CP) system.

The two main components of CP systems are the cyber structures [at times known as computing structures—see Adam (2010)] and the physical processes. The "physical process is [typically] monitored or controlled by the cyber system, which is a networked system of several tiny devices with sensing, computing and communication (often wireless) capabilities" (Wang et al. 2010, p. 733). The dependency on the cyber component, which includes both the hardware and software, allows for greater connectivity with other components of the system, thereby promoting interoperability (Adam 2010; Energetics Incorporated 2012). The physical component could be natural (e.g., volcano), man-made (e.g., surgical room), or a combination of both structures (Wang et al. 2010). These components work together to monitor the behavior of the physical processes, and initiate remedial actions to align their operations to work effectively and efficiently.

As these physical systems typically manage critical national resources and infrastructure, they are highly prized targets of attacks. While such assaults usually require perpetrators to be physically proximate, the presence of the cyber component in CP systems facilitates remote attacks, thereby increasing security risks (Energetics Incorporated 2012). Cardenas et al. (2009) state that "cyber-attacks are a natural progression to physical attacks: they are cheaper, less risky for the attacker, are not constrained by distance, and are easier to replicate and to coordinate" (p. 2). As such, it is not surprising that the US Department of Homeland Security (2012) had indicated a huge increase in the number of cyber attacks on industrial control systems over the last few years—there were 198 reported incidents in 2011, 41 in 2010, and nine in 2009. While the majority of these reported incidents occurred in the energy sector, the other sectors were not spared. In 2009, it was reported that hackers broke into the "air traffic control mission-support systems of the U.S. Federal Aviation Administration (FAA) several times" (Mills 2009, para. 1), and stole personal data pertaining to 48,000 of its current and past employees as well as passwords from servers connected with FAA's, and also planted malicious code which had the potential to shut down the system.

Technological advancements have been frequently hailed as the main safeguard for CP systems (Adam 2010; Energetics Incorporated 2012; Pasqualetti et al. 2013; Richards 2009; US Department of Homeland Security 2012; Wang et al. 2010). Wang et al. (2010) have listed three main sources of risk to CP security which would require a high level of technical expertise, namely skilled hackers, criminal groups, and state sponsored terrorist groups, which would, in turn, necessitate sophisticated technological protective responses. However, insiders such as employees and

business associates, who typically do not possess high-tech background, have also been listed as sources of risk. The US Department of Homeland Security (2012) reported that spear-phishing, in which "emails were convincingly crafted and appeared to be from corporate executives or other trusted sources in an attempt to lure users into opening malicious attachments or links" (p. 6), accounted for 41 % of the reported cyber-attack incidents, with a particular incident involving an infection from a small removable storage device. Operators of CP systems may also be deceived to take an action which is not required, or by not taking a required action, when detection mechanisms have been tampered with (Wang et al. 2010). The US Department of Homeland Security (2012) states that cyber security gaps occur when organizational personnel do not appreciate the security risks, or do not adhere to internal security policies, or when there is a lack of security policies within the organization. For example, measures such as changing passwords and usernames, and using of firewalls with VPN protection would do much to prevent cyber security lapses.

However, CP systems have proliferated such that they are present in everyday life and situations, having spread beyond organizational usage (Leavitt 2010; Pasqualetti et al. 2013; Rajkumar et al. 2010). In the United States alone, almost 2.6 million people rely on implanted medical devices which have a physical component that reads the person's health-related statistics and a cyber component that stores, computes, and communicates such valuable data to clinicians. This facilitates remote health monitoring of patients and could be used to actuate a response through the physical component (Energetics Incorporated 2012; Leavitt 2010; Wang et al. 2010). Intruders "could break into [these devices'] communications and either send harmful commands to the devices or steal private patient information" (Leavitt 2010, p. 11). In some cases, these devices perform life-supporting functions, and the possibility of such devices being tampered with would lead to adverse consequences (Energetics Incorporated 2012). For example, fatal jolts of electricity could be delivered to wirelessly connected heart defibrillators and pacemakers, or lethal amounts of insulin remotely injected into unsuspecting users (Feder 2008; Kostadinov n.d.). Besides healthcare equipment, society is beginning to see more robotic assistive devices, in the form of CP systems, for the elderly (Energetics Incorporated 2012). Rajkumar et al. (2010) claimed that "as the percentage of people over 65 in the population of the United States and elsewhere continues to increase, teleservices and assistive devices, [classified as CP systems], will play an ever-increasing role in providing home, assisted living and hospital services, prevention of falls, injury mitigation, and a host of other services" (p. 4). To take another example, modern cars have embedded CP systems which serve to enhance the driving experience via greater safety and convenience (Energetics Incorporated 2012; Koscher et al. 2010). Yet, Koscher et al. (2010) demonstrated that malicious hackers could remotely disable the brakes, stop the engine and manipulate the air bag deployment mechanism, thereby compromising safety. According to Symantec Corporation (2014), "baby monitors, as well as security cameras and routers, were

famously hacked in 2013" (p. 7), which reinforces how ubiquitous and vulnerable CP systems are. With the push towards 'smart infrastructure', CP system-enabled residences and wearable CP devices are becoming more common as well (Adam 2010; Energetics Incorporated 2012; Hoe and Hussain 2015; Rajkumar et al. 2010).

This chapter has shown that while technology provides some measure of protection for CP systems, non-technological solutions should be highlighted too, as human factors are a major source of CP security threats (Symantec Corporation 2014). Moreover, as CP systems gain in sophistication and are increasingly adopted for mass usage, society needs to be prepared to handle them. As such, the next section examines initiatives to build a culture that is conscious of technological security. Specifically, it explores educational efforts pertaining to CP security issues, and efforts to cultivate safe online practices. Singapore and Australia have been chosen as case studies.

11.2 Singapore

Singapore engages and continually pursues state-of-the-art technology for its critical national infrastructure projects, and employs various forms of CP systems (Chen-Khong and Tie 2013; Hoe and Hussain 2015; Lau et al. 2011; Lee 2007; Singapore Power 2015). Currently ranked first on the Networked Readiness Index compiled by the World Economic Forum, Singapore is also among the top ten in the world for its e-government initiatives, and seventh on the global list of tech-friendly cities (Karake-Shalhoub and Al Qasimi 2010; Lim 2015; World Economic Forum 2015). Moreover, with a high Internet penetration rate (with 87 % of its population having broadband access), Singapore has been touted as one of the most wired nations in the world (Infocomm Development Authority of Singapore n.d.-a; Karake-Shalhoub and Al Qasimi 2010). With a mobile penetration rate of 156 % and widespread access to wireless, location-based, cloud computing, and always-on technologies, the usage of Internet-connected devices is becoming pervasive in daily life (Infocomm Development Authority of Singapore n.d.-c; Symantec Corporation 2013b). According to the 2013 Norton Report (Symantec Corporation 2013b), compared to the global average, Singapore has a higher percentage of mobile users who, being unaware of security solutions for their mobile devices, use their devices for work and play. They also claim that their organizations do not have policies on using personal devices for work. Also, compared to the global average, there is a higher percentage of Singaporeans using public or unsecured Internet access. Moreover, BYOD (Bring-Your-Own-Device) policies have been increasingly adopted by organizations in Singapore (Infocomm Development Authority of Singapore n.d.-b). These statistics, along with recent hacking incidents targeted at the Singapore government, highlight the importance of addressing CP security in Singapore, and makes the country a suitable case study (Marsh 2014).

11.2.1 Educational Efforts

The National Cyber Security Masterplan 2018 (NCSM2018) is the government's strategic guide to improving cyber security (Infocomm Development Authority of Singapore, n.d.-b). Beyond enhancing the technological capabilities of the government agencies and critical national infrastructure, NCSM2018 seeks to raise awareness of cyber security among businesses and individuals through the Cyber Security Awareness and Outreach program. This program focuses on conveying security awareness messages and advisories via online videos, national television programs, and other communication channels to reach out to businesses and individuals (Infocomm Development Authority of Singapore n.d.-b). SingCERT, which is a program run by the Infocomm Development Authority of Singapore, is responsible for disseminating "timely information and alerts on the latest violation security issues to the general public via SingCERT website and SingCERT Mailing List" (SingCERT n.d. "What services does SingCERT provide", para. 1). With "the number of cyber security professionals [comprising] less than 1 % of the total infocomm industry workforce in Singapore" (Infocomm Development Authority of Singapore n.d.-b, p. 16), the NCSM2018 also endeavors to raise the number and competencies of cyber security experts through research and development, training, and testing programs (Marsh 2014). Through the Infocomm Development Authority of Singapore, the Cyber Security Awareness Alliance, which consists of like-minded government agencies, and private and public sector organizations, was formed to promote a healthy cyber security culture and awareness of such issues. Recognizing that a multi-pronged approach is required to raise awareness of cyber security issues and demonstrating its resolve, the Inter-Ministry Cyberwellness Steering Committee, consisting of many inter-governmental agencies, such as Ministry of Communication and Information, Ministry of Education, Ministry of Social and Family Development, Ministry of Defence, Ministry of Home Affairs, Infocomm Development Authority of Singapore, Media Development Authority of Singapore, and Health Promotion Board and National Library Board, was established in 2009 (Media Development Authority of Singapore n.d.). These collaborations would arguably prevent duplication of efforts, optimize resource usage, and enable a wider reach of the cyber security education efforts.

Beyond the government's efforts, promoting safe Internet habits has also been the thrust of various organizations involved in educating the masses on cyber security issues. Fei Yue Community Services, Kingmaker Consultancy, and TOUCH Community Services are prominent organizations that promote cyber safety by giving talks and conducting seminars for parents and children (Fei Yue Community Services n.d.; Kingmaker Consultancy n.d.; TOUCH Cyber Wellness n.d.). These talks and seminars are typically meant for the public and conducted through the public schools in Singapore. While the attendees are charged for the talks, these charges are lowered significantly or even waived entirely due to school or government subsidies.

11.2.2 Cultivating Safe Online Practices

The use of government e-services requires every citizen to have a password called the SingPass (Singapore Government n.d.). Each password has to adhere to the requirement of having 8–24 alphanumeric characters. While this is a common condition for passwords, the Singapore government further enhances the security level by also requiring users to "change their password every 2 years" (Singapore Government, n.d. "Security Enhancements for SingPass," para. 4). Moreover, failed login attempts would prompt the user to enter a generated code. This login requirement is not unique to the government sector, as the private organizations practice it as well. The National University of Singapore (NUS) adopts a stringent password policy for the users of its NUS network, with four other stipulations besides the minimum 8-character condition. Since early 2009, user passwords "must contain at least a number, an alphabet and a symbol (e.g. Pa55Word!), [must be changed] every 180 days, [can only be changed] at most once/day, [and users] cannot re-use any of [their] 6 previous passwords" (National University of Singapore, n.d. para. 3). Major banks in Singapore have also adopted a 2-Factor Authentication (2FA) login feature (Monetary Authority of Singapore n.d.). The first factor of identification is something the user knows, in this case, a personal identification number (PIN) or password. The second factor of identification is a token that the user possess, which is typically issued by the banks upon registration for their Internet banking services. During the login process, a user has to key in the PIN or password, as well as a one-time password generated by the 2FA token. While it may seem inconvenient, such measures undoubtedly go a long way in improving the security consciousness of users when dealing with cyber systems.

As the Singapore government increases the country's reliance on technology, it has engaged many stakeholders in creating a culture of security awareness (Hoe and Hussain 2015; Jiow 2013). The recent Annual Crime Brief 2014 released by the Singapore Police Force, in which social engineering type of cybercrimes saw an increase of 140 % compared to previous years, strongly suggests that while technological safeguards might be in place, the biggest security loophole lies in the people themselves (Hoe and Hussain 2015; Singapore Police Force n.d.). Singapore would do well to put more effort into public education on CP systems security to warn them against deceptive practices.

11.3 Australia

Much as in Singapore, Australia has a high Internet and mobile penetration rate. In 2013, there were more than 12–17.3 million subscribers for Internet and mobile handsets, respectively, in Australia (Australian Government: Attorney-General's Department 2013). According to a national survey, Australian businesses suffered financial losses amounting to at least AUD$595 million in the 2006–07 financial

year, and more than AUD$1.37 billion was spent annually to protect Australian businesses against computer security incidents (Richards 2009). In 2013, "the Australian Signals Directorate responded to 940 cyber incidents involving Government agencies, a 37 % increase on the previous year" (Prime Minister of Australia: The Hon Tony Abbott MP 2014, para. 8). The Cyber Crime and Security Survey Report 2013 found the worrying trend that "only 27 % of organizations had increased expenditure on IT security in the previous 12 months—a decrease of 25 % from 2012" (CERT Australia 2013, p. 4). The report also found that most of the cyber security incidents were the result of staff not being conscious of security issues and protocols. It is no surprise that cyber security has been touted as a "strategic priority for Australia's national security" (Parliament of Australia, n.d. "Key issue," para. 1).

11.3.1 Educational Efforts

The Australian Cyber Security Centre (ACSC) congregates all governmental cyber security resources to counter such threats (Australian Cyber Security Centre n.d.). ACSC serves both the private and public sectors by sharing information on cyber security threats, whereas CERT Australia serves Australian businesses by acting as the government's single contact point (Australian Federal Police n.d.; Australian Government: Attorney-General's Department n.d.). Stay Smart Online, SCAMWatch, and CyberSmart are notable initiatives by the Australian government to serve the general public in the area of education of cyber security issues (Australian Communications and Media Authority n.d.; Australian Competition and Consumer Commission n.d.; Australian Government Department of Communications n.d.). CyberSmart provides both online and onsite outreach efforts which include online presentations and virtual classrooms on cyber security issues, as well as workshops for parents and teachers on Internet safety. While CyberSmart tends to be comprehensive in its coverage of Internet safety issues, Stay Smart Online focuses on the protection of personal and financial information online, and SCAMWatch specifically on fraud cases and scams (Australian Competition and Consumer Commission n.d.; Australian Government Department of Communications n.d.). Stay Smart Online sends out timely information to its subscribers alerting them to security threats, a unique feature which serves to increase security consciousness.

Much like CyberSmart in its coverage of Internet safety issues, the ThinkUKnow program is a rare example of government partnerships with the private sector, with several police forces partnering with commercial companies (ThinkUKnow Australia n.d.). Other nongovernmental organizations that run such programs include Internet Education and Safety Services, and Raising Children Network (Internet Education and Safety Services n.d.; Raising Children Network n.d.). Such involvement of both private and public sectors in educational efforts indicates the importance of CP security to the various stakeholders. Yet, it is apparent that more stakeholders need to get involved as the demand for such educational programs exceeds the supply (Australian Communications and Media Authority n.d.;

Australian Government: Department of the Prime Minister and Cabinet n.d.). In contrast, Singapore appears to have ample supply of educational programs.

11.3.2 Cultivating Safe Online Practices

Access to many Australian government services requires an account known as myGov. The myGov passwords are required to be "at least 7 characters long and have at least one number" (Australian Government n.d.). Beyond myGov password requirements, a cursory exploration of account management policies shows that, while many Australian universities do provide instructions on how to choose a secure password, their other stipulations are less rigorous (for example, as in the frequency of changing passwords) compared to universities in Singapore (Australian National University n.d.; Murdoch University n.d.; Nanyang Technological University n.d.; National University of Singapore n.d.; The University of Melbourne n.d.; The University of Queensland n.d.). Moreover, banks in Australia typically do not require a 2FA process for its personal online banking services. Instead, a code generated and communicated via SMS to the user would suffice (Commonwealth Bank of Australia n.d.; National Australia Bank n. d.; Westpac Banking Corporation n.d.). Yet, Trend Micro (2013) claims that soon "basic two-step verification will no longer be sufficient" (p. 2).

Evidently, the Australian government recognizes the importance of CP security, and it is currently (in 2015) embarking on a comprehensive cyber security review (Australian Government: Department of the Prime Minister and Cabinet n.d.). While this review focuses on improving technological structures, mainly targeted at government and private sectors, and strengthening intra and international collaborations, it would do well to strengthen initiatives directed at the general public, as CP systems continue to aggressively proliferate.

11.4 Summary and Conclusions

This chapter started out by showing how CP systems have evolved on two fronts. First, CP systems, which conventionally referred to systems embedded in critical infrastructures, have seen widespread adoption in society at large. Second, the security of CP systems increasingly warrants non-technological solutions pertaining to how the average person uses the CP systems, beyond the technical solutions that have been frequently fore grounded. Two particular efforts were considered in this chapter—cyber security education and cultivation of safe online practices, and specifically, examining the login and password requirements. Two particular countries were selected as case studies due to their highly wired and connected populations.

Being far from exhaustive in its scope, this chapter proposes a few avenues for future studies. Firstly, though it is argued here that banking, tertiary institutional and government e-services login and password practices would reflect efforts in cultivating basic CP security habits, it is likely that the additional examination of firewall deployment by home owners and policies for Internet use would further inform this study. Secondly, future studies would elucidate this topic further by capturing the scope and depth of the educational programs offered, the programs' reach and their effectiveness. Comparatively, Australia's efforts and initiatives in CP system security appear lacking when compared to Singapore's, yet Australia's cybercrime rate is lower than Singapore's, and in fact is below the global average (Symantec Corporation 2013a, b). As such, comparative studies between more countries would advance this discourse, this being the third suggestion of avenues for future studies.

A comprehensive view of national efforts in improving CP systems security necessitates detailed information on the countries' educational efforts and a thorough look at initiatives (and/or policies) that cultivate relevant habits for CP system security. Yet, this chapter is significant as it focuses on non-technological efforts and initiatives in CP system security. Also, this chapter marks a relevant step in charting the directions for future conversations on CP systems security solutions—a crucial issue that is assuming growing importance in this "Internet of Things" era.

References

Adam, N. (2010). Workshop on future directions in cyber-physical systems security. Department of Homeland Security.

Australian Communications and Media Authority. (n.d.). CyberSmart. Retrieved April 17, 2015 from http://www.cybersmart.gov.au/.

Australian Competition and Consumer Commission. (n.d.). SCAMWatch. Retrieved April 17, 2015 from http://www.scamwatch.gov.au.

Australian Cyber Security Centre. (n.d.). Australian cyber security centre. Retrieved January 26, 2015 from http://www.acsc.gov.au/.

Australian Federal Police. (n.d.). High tech crime. Retrieved January 26, 2015 from http://www.afp.gov.au/en/policing/cybercrime/hightech-crime.aspx.

Australian Government. (n.d.). Security. Retrieved April 18, 2015 from http://www.my.gov.au/mygov/content/html/security.html.

Australian Government Department of Communications. (n.d.). Stay smart online. Retrieved April 17, 2015 from http://www.staysmartonline.gov.au.

Australian Government. (2013). *Attorney-General's Department*. National plan to combat cybercrime: Achieving a just and secure society.

Australian Government: Attorney-General's Department. (n.d.). Computer emergency response team. Retrieved January 26, 2015 from http://www.cert.gov.au/.

Australian Government: Department of the Prime Minister and Cabinet. (n.d.). Australian government's cyber security review. Retrieved April 18, 2015 from http://www.dpmc.gov.au/pmc/about-pmc/core-priorities/national-security-and-international-policy/australian-governments-cyber-security-review.

Australian National University. (n.d.). Login & Passwords. Retrieved April 18, 2015 from http://itservices.anu.edu.au/login-and-passwords/.

Cardenas, A. A., Amin, S., Sinopoli, B., Giani, A., Perrig, A., & Sastry, S. (2009). *Challenges for securing cyber physical systems.* Paper presented at the Workshop on Future Directions in Cyber-physical Systems Security.

CERT Australia. (2013). Cyber crime & security survey report.

Chen-Khong, T., & Tie, L. (2013). Sensing-driven energy purchasing in smart grid cyber-physical system. *Systems, man, and cybernetics: Systems, IEEE transactions on, 43*(4), 773–784. doi:10.1109/TSMCA.2012.2224337.

Commonwealth Bank of Australia. (n.d.). Online security. Retrieved April 18, 2015 from http://www.commbank.com.au/personal/netbank/online-security.html?ei=gsa_generic_online-security.

Energetics Incorporated. (2012). *Cyber-physical systems: Situation analysis of current trends, technologies, and challenges*. Retrieved from http://events.energetics.com/NIST-CPSWorkshop/pdfs/CPS_Situation_Analysis.pdf.

Feder, B. J. (2008). A heart device is found vulnerable to hacker attacks, *The New York Times*. Retrieved from http://www.nytimes.com/2008/03/12/business/12heart-web.html?_r=2 &.

Fei Yue Community Services. (n.d.). Fei Yue Community Services. Retrieved March 28, 2015 from http://www.fycs.org/.

Hoe, P. S., & Hussain, A. (2015). S'pore 7th highest in Asia-Pac for social media scams, *The Straits Times,* p. 5.

Infocomm Development Authority of Singapore. (n.d.-a). Household access to internet 2003–2013. Retrieved January 14, 2015 from http://www.ida.gov.sg/Infocomm-Landscape/Facts-and-Figures/Infocomm-Usage-Households-and-Individuals - 4.

Infocomm Development Authority of Singapore. (n.d.-b). The National Cyber Security Masterplan 2018. Retrieved December 27, 2014 from www.ida.gov.sg/Programmes-Partnership/Store/National-Cyber-Security-Masterplan-2018.

Infocomm Development Authority of Singapore. (n.d.-c). Telecommunications: Facts & figures. Retrieved December 27, 2014 from http://www.ida.gov.sg/Infocomm-Landscape/Facts-and-Figures/Telecommunications–1.

Internet Education and Safety Services. (n.d.). Internet education and safety services. Retrieved April 20, 2015 from http://www.iness.com.au/.

Jiow, H. J. (2013). Cyber crime in Singapore: An analysis of regulation based on Lessig's four modalities of constraint. *International Journal of Cyber Criminology, 7*(1), 18–27.

Karake-Shalhoub, Z., & Al Qasimi, L. (2010). *Cyber law and cyber security in developing and emerging economies*. Cheltenham: Edward Elgar Publishing.

Kingmaker Consultancy. (n.d.). Kingmaker Consultancy. Retrieved March 28, 2015 from http://kingmaker.com.sg/.

Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S.et al. (2010, May). *Experimental security analysis of a modern automobile.* Paper presented at the IEEE Symposium on Security and Privacy Berkeley, CA.

Kostadinov, D. (n.d.). H@acking implantable medical devices. Retrieved March 28, 2015 from http://resources.infosecinstitute.com/hcking-implantable-medical-devices/.

Lau, J. K.-S., Tham, C.-K., & Luo, T. (2011). *Participatory cyber physical system in public transport application*. Paper presented at the Fourth IEEE International Conference on Utility and Cloud Computing, Melbourne. http://www1.i2r.a-star.edu.sg/~luot/pub/%5BUCC11%5D-Participatory-Sensing-CPS-Transport.pdf.

Leavitt, N. (2010). Researchers fight to keep implanted medical devices safe from hackers. *Computer, 43*(8), 11–14. doi:10.1109/MC.2010.237.

Lee, E. A. (2007). *Computing foundations and practice for cyber-physical systems: A preliminary report*. Berkeley, CA: University of California.

Lim, A. (2015, March 23). S'pore No. 7 on global list of tech-friendly cities, *The Straits Times*. Retrieved from http://www.straitstimes.com/archive/monday/premium/money/story/spore-no-7-global-list-tech-friendly-cities-20150323–sthash.JSGKBFSh.dpuf.

Marsh. (2014). Cybercrime in Asia: A changing regulatory environment.

Media Development Authority of Singapore. (n.d.). Inter-Ministry Cyberwellness Steering Committee. Retrieved March 27, 2015 from http://www.mda.gov.sg/PublicEducation/MediaLiteracy/Pages/MediaLiteracy.aspx.

Mills, E. (2009, May 7). Hackers broke into FAA air traffic control systems, *CNET*. Retrieved from http://www.cnet.com/news/report-hackers-broke-into-faa-air-traffic-control-systems/.

Monetary Authority of Singapore. (n.d.). Understanding two-factor authentication and transaction signing. Retrieved April 13, 2015 from http://www.mas.gov.sg/moneysense/understanding-financial-products/investments/consumer-alerts/understanding-two-factor-authentication-and-transaction-signing.aspx.

Murdoch University. (n.d.). Murdoch password help. Retrieved April 18, 2015 from http://our.murdoch.edu.au/IT/Access-and-passwords/Login-at-Murdoch/Murdoch-Password/Murdoch-Password-help/—changepasswd.

Nanyang Technological University. (n.d.). New student. Retrieved April 18, 2015 from http://www.ntu.edu.sg/cits/newusers/newstudent/Pages/password.aspx.

National Australia Bank. (n.d.). Online security. Retrieved April 13, 2015 from http://www.nab.com.au/personal/internet-banking/security.

National University of Singapore. (n.d.). Update to NUSNET password policy. Retrieved April 13, 2015 from http://www.nus.edu.sg/comcen/gethelp/guide/itcare/Update to NUSNET Password Policy.pdf.

Parliament of Australia. (n.d.). Cyber security. Retrieved February 6, 2015 from http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BriefingBook44p/Cyber.

Pasqualetti, F., Dorfler, F., & Bullo, F. (2013). Attack detection and identification in cyber-physical systems. *Automatic Control, IEEE Transactions on, 58*(11), 2715–2729. doi:10.1109/TAC.2013.2266831.

Prime Minister of Australia: The Hon Tony Abbott MP. (2014). Cyber security review. Retrieved April 21, 2015 from http://www.pm.gov.au/media/2014–11-27/cyber-security-review-0.

Raising Children Network. (n.d.). Raising Children Network. Retrieved April 17, 2015 from http://raisingchildren.net.au/.

Rajkumar, R., Insup, L., Lui, S., & Stankovic, J. (2010). *Cyber-physical systems: The next computing revolution.* Paper presented at the Design Automation Conference, Anaheim, CA.

Richards, K. (2009). The Australian business assessment of computer user security: A national survey. In K. Richards (Ed.). *Research and Public Policy Series* (Vol. 102). Australian Institute of Criminology.

Singapore Government. (n.d.). Singpass. Retrieved April 13, 2015 from http://www.singpass.gov.sg/sppubsvc/.

Singapore Police Force. (n.d.). Annual crime brief 2014. Retrieved February 3, 2015 from http://www.spf.gov.sg/stats/crimebrief2015.html.

Singapore Power. (2015). About SP PowerGrid. Retrieved February 14, 2015 from http://www.singaporepower.com.sg/irj/portal?NavigationTarget=navurl://7d33724dfa9cf671e4314064deccb86e& windowId=WID1423881503391.

SingCERT. (n.d.). FAQ. Retrieved April 13, 2015 from http://www.singcert.org.sg/faq-topmenu-26 - A1.

Symantec Corporation. (2013a). Norton report 2013, Australia. Retrieved December 27, 2014 from http://www.symantec.com/content/en/us/about/presskits/b-norton-report-2013-australia.pdf.

Symantec Corporation. (2013b). Norton report 2013, Singapore. Retrieved December 27, 2014 from http://www.symantec.com/content/en/us/about/presskits/b-norton-report-2013-singapore.pdf.

Symantec Corporation. (2014). Internet security threat report 2014 (Vol. 19).

The University of Melbourne. (n.d.). Infrastructure services—IT. Retrieved April 18, 2015 from https://its.unimelb.edu.au/.

The University of Queensland. (n.d.). UQ password guide. Retrieved April 18, 2015 from http://www.its.uq.edu.au/helpdesk/uq-password-guide.

ThinkUKnow Australia. (n.d.). ThinkUKnow. Retrieved April 17, 2015 from http://www.thinkuknow.org.au/.

TOUCH Cyber Wellness. (n.d.). TOUCH Cyber Wellness. Retrieved March 28, 2015 from http://www.touch.org.sg/touch_cyber_wellness.

Trend Micro. (2013). Blurring boundaries: Trend Micro security predictions for 2014 and beyond. Retrieved April 1, 2015 from http://about-threats.trendmicro.com/au/security-predictions/2014/blurring-boundaries/.

US Department of Homeland Security. (2012). ICS-CERT Incident Response Summary Report, 2009–2011: Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

Wang, E. K., Ye, Y., Xiaofei, X., Yiu, S. M., Hui, L. C. K.,et al. (2010, December). *Security issues and challenges for cyber physical system.* Paper presented at the International Conference on Cyber, Physical and Social Computing.

Westpac Banking Corporation. (n.d.). How we protect you. Retrieved April 18, 2015 from http://www.westpac.com.au/personal-banking/online-banking/security/how-we-protect-you/.

World Economic Forum. (2015). The Global Information Technology Report 2015: ICTs for Inclusive Growth.

Chapter 12
Cyber Security, Trust-Building, and Trust-Management: As Tools for Multi-agency Cooperation Within the Functions Vital to Society

Jyri Rajamäki

Abstract Functions vital to society, such as critical infrastructure protection (CIP) and public protection and disaster relief (PPDR), are increasingly dependent on networks, electricity, and data processing infrastructure. Incidents such as natural hazards and organized crime do not respect national boundaries. As a consequence, there is an increased need for European collaboration and information sharing related to CIP and PPDR communications and information exchange technologies and procedures. However, "trust" could be seen as the most important issue with regard to multi-agency cooperation. Cyber security should be seen as a key enabler for the development and maintenance of trust in the digital world. It is important to complement the currently dominating "cyber security as a barrier" perspective by emphasizing the role of "cyber security as an enabler" of new interactions and services—and recognizing that trust is a positive driver for growth. CIP and PPDR are becoming more and more dependent on unpredictable cyber risks. Everywhere present computing means that CIP and PPDR organizations do not know when they are using dependable devices or services and there are chain reactions of unpredictable risks. If cyber security risks are not made ready, CIP and PPDR organizations will face severe disasters over time. Investing in systems that improve confidence and trust can significantly reduce costs and improve the speed of interaction. From this perspective, cyber security should be seen as a key enabler for the development and maintenance of trust in the digital world.

Acronyms

CI	Critical infrastructure
CIP	Critical infrastructure protection
EU	European union
FICORA	Finnish communications regulatory authority
ICT	Information and communication technology

J. Rajamäki (✉)
Laurea University of Applied Sciences, Vanha Maantie 9, 02650 Espoo, Finland
e-mail: jyri.rajamaki@laurea.fi

R.M. Clark and S. Hakim (eds.), *Cyber-Physical Security*,
Protecting Critical Infrastructure 3, DOI 10.1007/978-3-319-32824-9_12

II	Information infrastructure
ISMS	Information security management system
KATAKRI	Finnish national security auditing criteria
PPDR	Public protection and disaster relief
PSC	Public safety communications
SIS	Software-intensive systems
TETRA	Terrestrial trunked radio

12.1 Introduction

In major disasters, not a single organization can work alone. Hence, cooperation is extremely critical between actors. The working parties should not simply trust and rely on their own resources. Regardless, only a few organizations possess all the required areas of expertise in a large-scale incident or disaster. Information sharing and education at the organizational level is required in order to achieve a working relationship between the actors. This requires actual and operational interoperability between the first-responding organizations—in reality in the field, not only in the form of an official agreement but on a much larger scale (Akella et al. 2010).

Critical infrastructure protection (CIP) is the analogous shared concern and responsibility of the society. Water, power, finance, Internet, transport, and all communication systems are part of the critical infrastructure (CI) and are essential to daily activities. Private industry owns and operates most of the CI assets, and the government serves as a regulator and consumer but often has a limited role. The various CI components are, to varying extent, dependent up-on one another within a country's borders and internationally. As such, problems in one CI component can quickly spread to others (George 2008). The operation of most CIs rests partly on their own dedicated communication systems as well as simultaneously on commercial networks.

The term 'public protection and disaster relief' (PPDR) is used to describe critical public services that have been created to provide primary law enforcement, firefighting, emergency medical services, and disaster recovery services for the citizens of the political subdivision of each country (Baldini 2010). In recent years, the capabilities of PPDR organizations across Europe have significantly improved with the deployment of new technologies, including dedicated TETRA (Terrestrial Trunked Radio) networks. Nevertheless, events like the London bombing in 2005, the Schiphol airport disaster in 2009 and the flooding disasters in 2010–11 have highlighted a number of challenges that PPDR organizations face in their day-to-day work. Secure and reliable wireless communication between first responders and their emergency control centers is vital for successful handling of every emergency situation. This also applies to each connected respondent and includes police, fire, medical or civil protection (Goldstein 2012).

CIP and PPDR actors have multiple similar needs. Lapierre (2011) suggests that similarities in disaster relief operation scenarios include (a) severe disruptions in expected functionalities of critical infrastructures, such as transport, supplies, and infrastructures; (b) operations in remote areas without transmission infrastructures; (c) cross-border operations and multinational teams; (d) high demand for interoperability; (e) a lack of remaining infrastructures after a serious disaster; (f) congestion or no use of commercial networks; and (g) utilization of both ad hoc networks and stable infrastructures. According to Lapierre (2011), similarities in command and control communications involve (1) a desire to obtain information on the operational environment, (2) a need for the decision maker to monitor operation (live feed), (3) a need to examine and issue orders, and (4) a desire to assess the progress of the operational environment after an order has been issued.

CIP and PPDR organizations increasingly face interoperability issues at all levels (technical, operational, and human) as they interact with other national, regional, or international organizations. Not only assets and standards must be shared across Europe but also collective responses to threats and crisis must be enabled in an increasingly interconnected network. In addition, the organizations stand to gain from the interoperability functionality in their routine work. On one hand, Europe is a patchwork of languages, laws, and diverse cultures and habits that can change abruptly across borders. On the other hand, even in the same country, each CIP and PPDR organization develops its own operational procedures. For efficient operations, many serious challenges need to be addressed, including critical governmental communication systems (which are not compatible even when they use the same technology) and differing procedures as well as inadequate language skills in cross-border cooperation.

CIP and PPDR operations are increasingly more dependent on information and communication technology (ICT) systems and services. Incidents such as natural hazards and organized crime do not respect national boundaries, but public protection and disaster relief operations are based on national organizations. As a consequence, there is an increased need for European collaboration and information sharing related to public safety communications (PSC) and information exchange technologies and procedures. European Union (EU) has funded dozens of research projects aiming toward better technological interoperability, but their results have been minor, because distrust—not technology—is the biggest problem to interconnect different organizations' ICT systems together (Kämppi et al. 2014).

12.2 Building Cyber-Trust

The purpose, with regard to security, is to know what is going on and what will happen in the network(s), and to be aware of the current level of security in the network(s), how to design or build-in security and resilience to a networked environment, and to define trade-offs for security and privacy levels versus system's usability (Ahokangas et al. 2014). The overall aim is to mitigate cyber security

Fig. 12.1 Themes of trust-building [adopted from (Ahokangas et al. 2014)]

risks, which in its turn supports the business continuity and operations of the whole society (DIGILE 2014).

Investing in systems that improve confidence and trust can significantly reduce costs and improve the speed of interaction. From this perspective, cyber security should be seen as a key enabler for the development and maintenance of trust in the digital world. Cyber security has the following four themes: (1) security technology, (2) situational awareness, (3) security management, and (4) resilience (Ahokangas et al. 2014), as shown in Fig. 12.1. Situational awareness is needed for having a correct understanding of security incidents, network traffic, and other important aspects that affect security; and security technologies are needed for protection (Ahokangas et al. 2014). Human aspects have to rule in via security management (Rajamäki and Rajamäki 2013). Consequently, resilient systems and infrastructures have the ability to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events (National Research Council 2012). Security audit is a way to demonstrate an organization's security level.

12.2.1 Resilience

The human body is inherently resilient in its ability to persevere through infections or trauma, but our society's critical infrastructure lacks the same degree of resilience, typically losing essential functionality following adverse events (Linkov et al. 2014). Without proper protection and development with cyber security in mind, modern society relying on critical infrastructures would be extremely vulnerable to accidental and malicious cyber threats. Resilient systems are able to minimize the negative impacts of adverse events on societies and sustain or even improve their functionality by adapting to and learning from fundamental changes caused by those events (Linkov et al. 2014).

The overall target of cyber security is that systems and infrastructures are resilient against all cyber incidents. In the case of information security, resilience

means that a system or infrastructure is able to adapt to changing conditions, based on runtime situational awareness and a priori risk analysis (Ahokangas et al. 2014). Resilience is based on integrating two parallel subtasks: (1) runtime situational awareness and (2) a priori risk analysis. On the other hand, resilience itself is a twofold topic: (1) the system has to be robust against attacks, i.e., the attack is prevented in its first phase, and (2) the system has to be able to return to a safe state after the attack. Healing requires that utilized data and system operation can be restored as soon as possible. Therefore, healing processes have to be trained and tested.

12.2.2 Situational Awareness

Situational Awareness is the main prerequisite toward cyber security. Without situational awareness, it is impossible to systematically prevent, identify, and protect the system from the cyber incidents and if, for example, a cyber-attack happens, to recover from the attack (Ahokangas et al. 2014). Situational awareness involves being aware of what is happening around your system to understand how information, events, and how your own actions affect the goals and objectives, both now and in the near future. It also enables to select effective and efficient countermeasures, and thus, to protect the system from varying threats and attacks.

Situational awareness is needed for creating a sound basis for the development and utilization of countermeasures (controls), where resilience focuses. The most important enablers of situational awareness are observations, analysis, and visualization, cyber-policy of the government as well as national and international cooperation. For the related decision-making, relevant information collected from different sources of the cyber environment or cyberspace, e.g., networks, risk trends, and operational parameters, are needed. This requires information exchange between different stakeholders. And always, when dealing with information exchange, the main question is “trust.”

12.2.3 Security Technology

Security technologies include all technical means toward cyber security, such as secure system architectures, protocols, and implementation, as well as tools and platforms for secure system development and deployment. Security technologies are needed for fulfilling the recognized security requirements, and for building resilient infrastructures and systems with dependable hardware and software that can also meet future security challenges (Ahokangas et al. 2014).

Security technologies enable technical protection of infrastructures, platforms, devices, services, and data. The technical protection starts with secure user identification and authorization that are necessary features in most secure infrastructures,

platforms, devices, and services. Fortunately, well-known technologies exist for their implementation. Typically, processes and data objects are associated with an owner, represented in the computer system by a user account, who sets the access rights for others. A global trend is to increase the use of cloud service technology when providing critical services. Data go into a cloud and will not come back to endusers' devices. Also, government data has already gone to a cloud, and in the future more and more government data will migrate to cloud servers and services. Partnerships between cloud service providers and security solution providers are becoming more common. We will see the emergence of cloud service-specific-solution providers as well. Identity management and encryption will be the most important cloud security services to be offered. These services will be eventually offered for small to medium-sized businesses as well. We will also see emergence of cloud security standards. Challenges are that quite often cloud service providers believe that security is just an end user issue and firewall means security. Therefore, currently, we do not have proper cloud security standards and we lack awareness of a true understanding of comprehensive cloud security (Ahokangas et al. 2014; DIGILE 2014).

Security technologies are needed also then if something has happened. For example, forensics can lead to the sources of the attack/mistake and provide information for legal and other ramifications of the issue. Forensics also facilitates the analysis of the causes of the incident, which in turn, makes it possible to learn and avoid similar attacks in the future.

12.2.4 Security Management and Governance

The well-known fact of life is that people are the rock-bottom of cyber security. Security management and governance, "the brain and Intelligence of cyber security" takes care the human and organizational aspects of cyber security.

Security policy is currently the main element used to communicate secure work practices to employees and ICT stakeholders. It is a declaration of the significance of security in the business of the organization in question. Additionally, the security policy defines the organization's policies and practices for personnel collaboration. However, people still often fail to comply with security policies, exposing the organization to various risks. One challenge is to promote methods and techniques that can support the development of comprehensible security policies in the emerging ICT paradigms, e.g., cloud computing and multiple devices (Ahokangas et al. 2014). Developing of policies that can defeat the main reasons driving non-compliance, such as a habit, is challenging.

Information security management system (ISMS) means continuously managing and operating system by documented and systematic establishment of the procedures and process to achieve confidentiality, integrity, and availability of the organization's information assets that do preserve (Lee and Jang 2009). ISMS provides controls to protect organizations' most fundamental asset, information.

Many organizations apply audits and certification for their ISMS to convince their stakeholders that security of organization is properly managed and meets regulatory security requirements (Broderick 2006). An information security audit is an audit on the level of information security in an organization. Security aware customers may require ISMS certification before business relationship is established. Unfortunately, ISMS standards are not perfect and they possess potential problems. Usually guidelines are developed using generic or universal models that may not be applicable for all organizations. Guidelines based to common, traditional practices take into consideration differences of the organizations and organization specific security requirements (Siponen and Willison 2009).

12.2.5 Security Audit

Many different types of audits exist, including financial audits, property assessments, supplier reviews, contractor evaluations, registration audits, and equipment evaluations (Russell 2012). Figure 12.2 illustrates internal (first-party) and external (second-party and third-party) auditing types. The common principle is that they compare applied procedures, as well as a set of collected information, against some established criteria.

ISO/IEC 17021-2 is a normative standard intended for use by accreditation bodies when assessing management systems, while ISO 19011 provides guidelines for first-, second-, and third-party auditors when auditing management systems. The third-party certification industry will use ISO 17021-2 to define requirements for

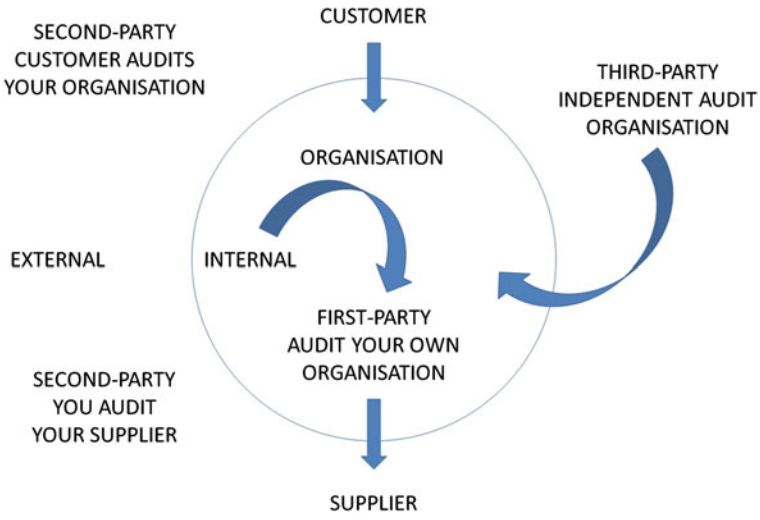


Fig. 12.2 First-second- and third-party audits [adapted from (Russell 2012)]

audits and audit arrangements and accreditation bodies will determine whether a certification body's auditing arrangements and activities comply with those requirements. ISO 19011 identifies best practice and provides information on what should be done when carrying out an audit without specifying how it must be done. ISO 19011:2011 edition includes an extension of the standard's earlier scope of application from quality and environmental management systems to all types of management systems auditing. Continuing development of management systems standards for information security, for example, means that ISO 19011 must be able to accommodate differing requirements while still providing useful guidance (Simpson 2010).

The three things that make a management system audit different from other types of assessments are that the audit must be (1) systematic, (2) independent, and (3) documented. In order to conduct systematic management system audits, there is a need for both audit procedures and an audit program. From an independence point of view, auditors cannot audit their own work or that of their colleagues,' as there would be a conflict of interest. Audits need to be structured, to ensure they are free from bias and conflicts of interest. Audits must be documented, because they are all about making decisions and taking action (Rajamäki and Rajamäki 2013).

The root of the Finnish National Security Auditing Criteria, KATAKRI is to preserve the confidentiality of any confidential and classified information held by the organization concerned. It is published by the Ministry of Defence, but Confederation of Finnish Industries, Finnish Communications Regulatory Authority (FICORA), Ministry of Foreign Affairs, and Ministry of the Interior have also participated in the preparation of the criteria. KATAKRI was officially published in 2009, update in 2011, and Version III was published in March 2015.

The National Security Auditing Criteria are mutual security criteria for officials and companies for unifying the communal security procedures and to improve self-monitoring and auditing. The National Security Auditing Criteria are an auditing tool used by the officials when carrying out inspections on the level of security within a company or a community. According to the current version of the criteria, KATAKRI's main goal is to harmonize official measures when an authority conducts an audit in a company or in another organization to verify their security level. The Finnish National Security Authority uses KATAKRI as its primary tool when checking the fulfillment of security requirements. The preface to the criteria states that the second important goal is to support companies and other organizations, as well as authorities and their service providers and subcontractors, in working on their own internal security. For that reason, the criteria contain recommendations for the industry that are separate and outside of the official requirements; it is hoped that useful security practices will be chosen and applied, thus progressing to the level of official requirements.

The Finnish National Security Auditing Criteria, KATAKRI are divided into three main areas: (1) administrative and personnel security, (2) physical security, and (3) information security. Areas are not meant to be used independently. It is instructed to take all three areas into account when performing accreditation audit using KATAKRI.

12.3 Resilient Software-Intensive Systems

Theory of complex systems traces its roots to the 60s when Herbert A. Simon wrote his book "Science of the Artificial" (Simon 1978). Fulfillment of purpose involves the relationship between the artifact, its environment and a purpose or goal. Alternatively, it can be viewed as the interaction of an inner environment (internal mechanism), an outer environment (conditions for goal attainment) and the interface between the two. According to Hevner and Chatterjee (2010), the real nature of the artifact is the interface. Both the inner and outer environments are abstracted away. The science of artificial complex systems should focus on the interface, the same way design focuses on the "functioning." According to Hevner and Chatterjee (2010), a general theory of complex systems must refer to a theory of hierarchy, and the near-decomposability property simplifies both the behavior of a complex system and its description.

Revolutionary advances in hardware, networking, information, and human interface technologies require new ways of thinking about how software-intensive systems (SIS) are conceptualized, built, and evaluated. According to Hevner and Chatterjee (2010), manual methods of software and systems engineering must be replaced by computational automation that will transform the field into a true scientific and engineering discipline. They also argue that the vision of science of design research for SIS must achieve the following essential objectives:

- *Intellectual amplification: Research must extend the human capabilities (cognitive and social) of designers to imagine and realize large-scale, complex software-intensive systems.*
- *Span of control: Research must revolutionize techniques for the management and control of complex software-intensive systems through development, operations, and adaptation.*
- *Value generation: Research must create value and have broad impacts for human society* via *the science and engineering of complex software-intensive systems and technologies.*

Figure 12.3 illustrates the three layers of SIS: (1) the platform layer, (2) the software layer, and (3) the human layer, and the two critical interfaces between these layers. Also, concepts of the software layer are shown on the right side of the figure. According to Hevner and Chatterjee (2010), the software layer is a makeup of software code, information, and control within the context of an application domain. They continue that "the overlaps among these three concepts support varying methods and techniques of understanding and building the software layer of systems. For example, software architectures define structures for integrating the concept of code, information, and control for a particular application domain system."

SIS design entails many important decisions, such as the design and allocation of system behaviors (e.g., functions, actions) and system qualities (e.g., performance, security, reliability) to the different layers (Hevner and Chatterjee 2010). A particular system activity could be realized in hardware (platform), via, for

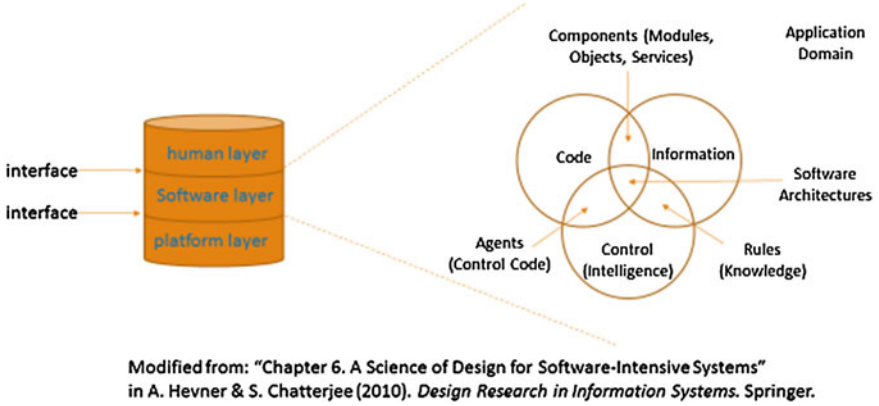


Fig. 12.3 Software-intensive systems

example, a service call (software), by human behavior (human) or by some combination of activities across all three layers, and a performance requirement (e.g., response time) for an SIS transaction could be divided and allocated as performance requirements in each of the layers (Hevner and Chatterjee 2010). Nearly, all future SIS will be connected to environmental resources and other systems via network connections, and these connections lead to complex systems-of-systems architectures to provide behaviors and qualities (Hevner and Chatterjee 2010). There will be identifiable networks across all three SIS layers: physical networks support the transmission of digital and analog data among system platforms, software networks provide the middleware layers, and protocols that transform the transmitted data into information that is shared among the information processing systems, and social networks provide a means of interaction and community among the human participants of the complex system (Fiadeiro 2007).

12.3.1 Design Principles for Information Infrastructures

The information infrastructure (II) literature has addressed the challenges of realizing large-scale technological systems (Hanseth and Lyytinen 2010; Monteiro and Hanseth 1996; Star and Ruhleder 1996; Edwards et al. 2009). Large-scale information systems are not stand-alone entities but rather are integrated with other information systems and communication technologies as well as with other technical and nontechnical elements. This approach is relevant for analyzing the domain of critical information infrastructures.

Hanseth and Lyytinen (2010) have synthesized their study's insights into a normative design theory for IIs, distinguishing between two generic challenges: (1) The "bootstrap problem" addresses the establishment of a novel II. Since an II gains much of its value from its large and diverse user base and components, the

fact that initially the user community is nonexistent or small precludes the fact that the infrastructure can offer these benefits. (2) The "adaptability problem" relates to the further growth and expansion of an II where unforeseen demands, opportunities, and barriers may arise.

Aanestad and Jensen (2011) have studied IIs in healthcare. According to them, large-scale and long-term stakeholder mobilization is a core challenge when realizing nationwide information infrastructures for public organizations. They continue that the implementation strategy of such IIs must deal with the multiple stakeholders and be able to mobilize and coordinate them. A modular implementation strategy, made possible by appropriate modularity of the solution, allows the implementation to be organized in a way that does not require wide-spread and long-term commitment from stakeholders initially. Aanestad and Jensen (2011) argue that "solutions that provide immediate use value by offering generic solutions to perceived practical problems, balance the stakeholders' costs and benefits, and solve a problem with minimal external dependencies, can avoid some of the dilemmas often associated with large-scale IIs." Their research illustrates the dangers of introducing requirements that are too high for stakeholder mobilization, and the notions of stable intermediary forms and modular transition strategies may help decision makers to pursue other avenues when planning large-scale implementation projects (Aanestad and Jensen 2011).

There has been a gigantic shift from a hardware product-based economy to one based on software and services (Hevner and Chatterjee 2010). This has also been the fact with regard to critical infrastructures as well as public protection and disaster relief. For example, the ICT systems of a typical police vehicle already cost about the half that of a new vehicle (Tikanmäki et al. 2014). From every indication, the growth of the software layer, in size and percentage of the overall systems, will be the future trend.

12.3.2 Systematic Design for Resilient SISs

According to Hevner and Chatterjee (2010), in the future world of pervasive computing and ubiquitous cyber-physical devices, it will be essential that IT artifacts and the integrated systems containing these artifacts be reliable, adaptable, and sustainable. Design for SIS should draw its foundations from multiple research disciplines and paradigms in order to effectively address a wide range of system challenges. According to Hevner and Chatterjee (2010), the most important intellectual drivers of future science of design in SIS research will be dealing with complexity, composition and control. Hanseth and Lyytinen (2010) adopt the viewpoint of designers: "how to 'cultivate' an installed base and promote its dynamic growth by proposing design rules for II bootstrapping and adaptive growth." Within their design rules, the II designers would have to prefer continuous, local innovation to increase chaos and to apply simple designs and crude abstractions. According to Hanseth and Lyytinen (2010), this change is not likely,

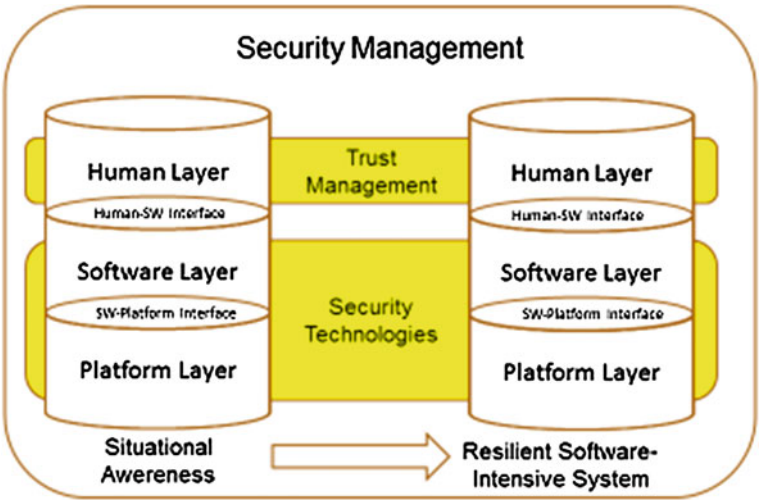


Fig. 12.4 Systematic approach toward resilient software-intensive systems (Rajamäki and Pirinen 2015)

as design communities are often locked into institutional patterns that reinforce design styles assuming vertical control and complete specifications.

Trustworthy and secure technologies and platforms are a basis to build on. As the security risks continue to increase with cybercrime and other unauthorized access, the security solutions and management of IT security need systematic design and constant development. Figure 12.4 shows the new systematic approaches toward resilient software-intensive systems. Security auditing standards and criteria are good tools when designing resilient systems. For example, Finnish National Security Auditing Criteria, KATAKRI, could be applied in all levels in Fig. 12.4: KATAKRI's *administrative security requirements* could be applied when assessing security management systems; KATAKRI's *personnel security requirements* when assessing human layer and trust-management systems; KATAKRI's *physical security requirements* when assessing the platform layer and the security technologies used there; and KATAKRI's *information security requirements* when assessing the software layer and the security technologies used there.

12.4 The Functions Vital to Society: A Complex Software-Intensive System

The functions vital to society consist of what keep the wheels of secure daily life turning. When the basic functions of society are in order it is possible to return to normal life after crises without losing the firm ground on which society rests. The

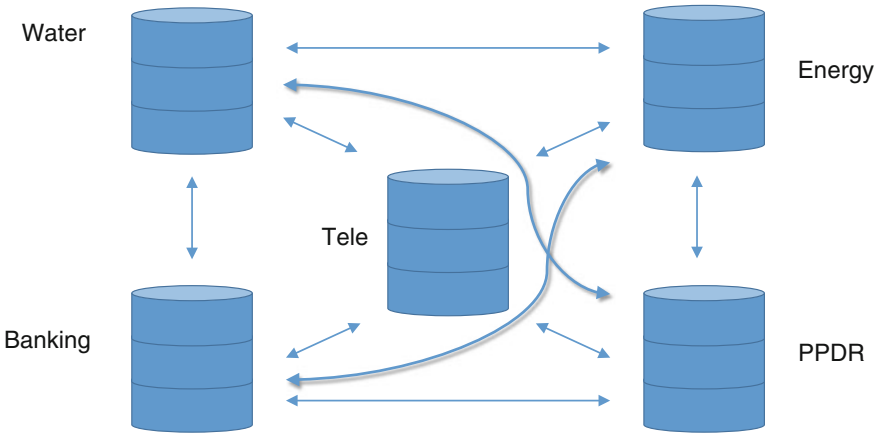


Fig. 12.5 A part of the complex SIS of the functions vital to society

importance of the functions vital to society becomes evident when something goes badly wrong; for example, an extensive power failure, or a major accident occurs. However, the functions vital to society must be secured in all times: in normal conditions as well as in crises.

From citizens' point of view, the functions vital to society belongs to one complex software-intensive system that consists of several different subsystems, such as a well-functioning financial and judicial systems, sufficient healthcare and public protection, and disaster relief, a clean living environment, smooth traffic, and resilient energy, water, and food supply. Figure 12.5 shows a part of the complex SIS of the functions vital to society.

All these subsystems are further divided to many sub-subsystems. This section proposes, how a cyber-secure complex SIS of the functions vital to society should be designed exploiting (1) general information security principles, (2) building cyber-trust and the systematic design principles for a resilient SIS presented in the previous sections, (3) the theory for designing complex SISs, and (4) the principles of the Finnish National Security Auditing Criteria, KATAKRI.

Information Security Handbook (US Code Title 44 2008) defines information security as follows: The term information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:

- *integrity*, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity,
- *confidentiality*, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information, and
- *availability*, which means ensuring timely and reliable access to and use of information.

Quite often, however, the *confidentiality* requirements of sub-subsystems are weighted today at the expense of information integrity and availability within the overall system. For that reason, critical information is not always available when needed. Usually, citizens meet this issue within the healthcare system, where service providers hide patients' critical health information keeping privacy protection as a pretext, although lack of cyber-trust designing of their information systems is the fundamental weakness.

The previous sections discuss how to return privacy and trust in digital world and to gain a global competitive edge in security-related business. The targets could be summarized as follows (Rajamäki and Knuuttila 2015):

1. Proactive—design for security. A proactive model of information security that is driven by knowledge of vulnerabilities, threats, assets, potential attack impacts, the motives, and targets of potential adversaries.
2. Self-healing—utilizing the toolbox. Novel and effective tools and methods to cope with challenges of dynamic risk landscape with self-healing.
3. Public awareness—increase trust. Enable seamless cyber security integration to everyday life. By efficiently utilizing tools and methods, stakeholders can cooperate while protecting their privacy, they can create more sophisticated security policies, media publicity can move from threats to opportunities and public awareness and understanding will move toward accepting cyber security as a natural element of a connected world.

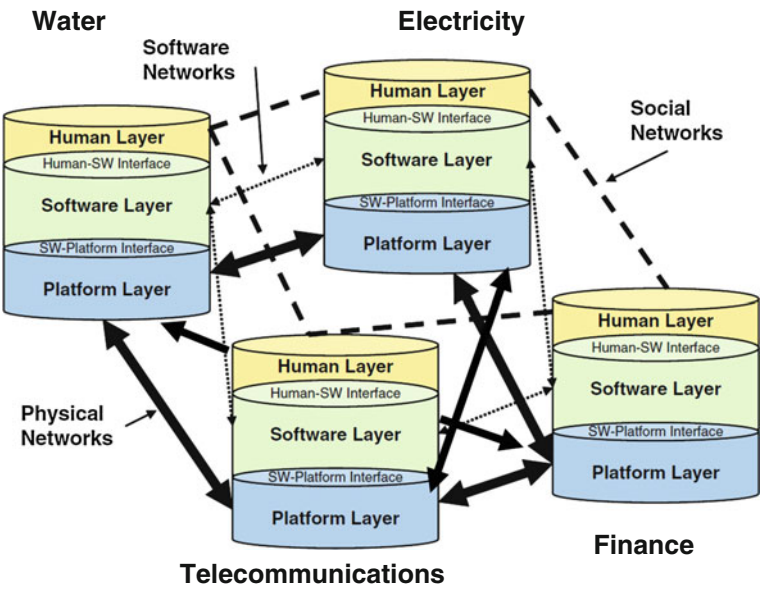


Fig. 12.6 Subnetworks of complex SIS model for Cis [adapted from (Hevner and Chatterjee 2010)]

Software-intensive systems consist of three layers: the platform layer, the software layer, and the human layer. Every cyber-secure system consists of two SISs: the proper resilient system, and the situational awareness system, that is, the main prerequisite toward cyber security. A complex SIS is a system of software-intensive subsystems, which platform layers compose a physical network, software layers compose a software network, and human layers compose a social network, as shown in Fig. 12.6. Trust should be systematically built up at all layers and networks. The resilient physical network is the basis on which the information sharing between different stakeholders could be created via software layers. However, the trust inside social networks quantifies the pieces of information that will be shared,—and with whom.

12.5 European Perspective

Europe has started major initiatives in ICT sectors for the growth of its digital economy (more recently: big data, cloud computing, Internet of Things, etc.) mainly on research-related issues. All these activities are envisaging "self-standing" security approaches, not benefitting from shared competences and solutions and not sufficiently leading to market implementation. A transversal security approach across these initiatives could increase efficiency and help the concrete use of European cyber security solutions for resilient systems, situational awareness, security technologies, and security management and governance. Such an overarching initiative should be complemented by a capability building roadmap leading EU and member states to invest in network and information systems security projects, thereby, bridging the gap between innovation and market and ensuring that other large initiatives, such as broadband networks, satellite communications, and EU wide large communication and information systems be properly protected.

Cyber security is the key enabler for the development and maintenance of trust in the digital world. The EU cyber security strategy was adopted by the EC in 2012 to drive development and application of cyber security solutions in Europe. However, the market for cyber security products is dominated by global suppliers and Europe is lagging behind. Shadowed by low efficiency, this is coupled with increasing issues including technological independence, sovereignty, legitimate privacy concerns, and market fragmentation (at EU and member state levels). Trust and information sharing across member states still remains a main concern in the development of an EU cyber security platform. CIP and PPDR agencies' present-day digital systems do not support cross-border cooperation. In addition to technical challenges, the distrust between agencies (especially in law enforcement, such as police) causes trouble. Unfortunately, this distrust also exist at the national level, and even between units of one organization. However, common digital systems and operational procedures could increase the trust between parties. A very important change is needed, where the mental-picture of cyber security should be changed from "threat, crime, attack" into "trust." Information security and

information security management system standards should be redeveloped toward a tool that encourages and simplifies the sharing of mission-critical data between CIP and PPDR actors.

Trustworthy and secure technologies and platforms are a basis to build on. As the security risks continue to increase with cybercrime and other unauthorized access, the security solutions and management of IT security need constant development and new approaches to keep up with the pace. Likewise, their successful use requires awareness and education. Research and education are the main drivers for complementing the currently dominating "cyber security as a barrier" perspective by emphasizing the role of "cyber security as an enabler."

The most efficient custom to increase cyber security is the improvement of know-how. Adaptive awareness and education processes are needed that can support users in all aspects of their evolving role in processing information using ICT. The cyber security strategies and development plans require the improvement of the know-how of actors in economic life and public administration. Continuous learning, using past experience, is a prerequisite for improving human behavior in organizations.

Most of the research and education in European universities combines security with some application area, e.g., computer networking or information systems, or links it to another field of science, such as mathematics and data mining. This broad perspective on security is essential for the long-term economic impact of the current security push. It would not make sense to produce a deluge of experts only in cyber security. Moreover, security has become a broad research topic that overlaps with many other areas of research. For example, software technologies and software engineering, computer networking, and data analysis are closely related to cyber security and are well represented at European universities and research institutions.

References

Aanestad, M., & Jensen, T. B. (2011). Building nation-wide information infrastructures in healthcare through modular implementation strategies. *The Journal of Strategic Information Systems, 20*(2), 161–176.

Ahokangas, M., Arkko, V., Aura, T., Erkinheimo, P., Evesti, A., Frantti, T., Hautamäki, J., Helenius, M., Hämäläinen, M., Kemppainen, J., Kirichencko, A., Korkiakoski, M., Kuosmanen, P., Laaksonen, M., Lehto, M., Manner, J., Remes, J., Röning, J., Sahlin, B., Savola, R., Seppänen, V., Sihvonen, M., Tsochou, A., Vepsäläinen, P. et al. (2014). Strategic research agenda for cyber trust. DIGILE.

Akella, R., Tang, H., & McMillin, B. M. (2010). Analysis of information flow security in cyber–physical systems. *International Journal of Critical Infrastructure Protection, 3*(3), 157–173.

Baldini, G. (2010). Report of the workshop on "Interoperable communications for safety and security". Publications Office of the European Union.

Broderick, J. S. (2006). ISMS, security standards and security regulations. *Information security technical report 11*(1), 26–31.

DIGILE 2014. In the pipeline: Cyber trust. Available in http://www.digile.fi/Services/researchprograms/cybertrust.

Edwards, P. N., Bowker, G. C., Jackson, S. J., & Williams, R. (2009). Introduction: An agenda for infrastructure studies. *Journal of the Association for Information Systems, 10*(5), 364–374.

Fiadeiro, J. L. (2007). Designing for software's social complexity. *IEEE Computer, 40*(1), 34–39.

George, R. (2008). Critical infrastructure protection. *International Journal of Critical Infrastructure Protection, 1*, 4–5.

Goldstein, M. L. (2012). *Emergency communications: Various challenges likely to slow implementation of a public safety broadband network GAO-12–343*. Washington, D.C.: United States Government Accountability Office.

Hanseth, O., & Lyytinen, K. (2010). Design theory for dynamic complexity in information infrastructures: the case of building internet. *Journal of Information Technology, 25*(1), 1–19.

Hevner, A. & Chatterjee, S. (2010). *Design science research in information systems*. Springer.

Kämppi, P., Rajamäki, J., Tiainen, S., & Leppänen, R. (2014). *MACICO—Multi-agent co-operation in cross-border operations*. Vantaa: Laurea.

Lapierre, G. (2011). *Synergies and challenges between defence and security (PPDR) applications*. What implication for the EU? Keynote presentation, PSC Europe Conference, Brussels.

Lee, W. & Jang, S. (2009). A study on information security management system model for small and medium enterprises. *Recent advances in e-activities, information security and privacy*, 84–87.

Linkov, I., Bridges, T., Creutzig, F., Decker, J., Fox-Lent, C., Kröger, W., et al. (2014). Changing the resilience paradigm. *Nature Climate Change, 4*, 407–409.

Monteiro, E. & Hanseth, O. (1996). Social shaping of information infrastructure: On being specific about the technology. *Information technology and changes in organizational work*, 325–343.

National Research Council (2012). *Disaster resilience: A national imperative*. The National Academies Press.

Rajamäki, J. & Knuuttila, J. (2015). *Cyber security and trust: Tools for multi-agency cooperation between public authorities*. Proceedings, 7th International Conference on Knowledge Management and Information Sharing (KMIS), Lisbon.

Rajamäki, J. & Pirinen, R. (2015). Critical *Infrastructure Protection: Towards a Design Theory for Resilient Software-Intensive Systems*. Proceedings, European Intelligence and Security Informatics Conference (EISIC), Manchester.

Rajamäki, J. & Rajamäki, M. (2013). *National Security Auditing Criteria, KATAKRI: Leading Auditor Training and Auditing Process*. 12th European Conference on Information Warfare and Security, Academic Conferences and Publishing International Limited, Reading, 217–223.

Russell, J. P. (2012). *The ASQ auditing handbook*. ASQ Quality Press.

Simon, H. (1978). *The science of the artificial*. Cambridge: MIT Press.

Simpson, P. (2010). ISO 19011 vs ISO/IEC 17021–2. The health and safety edition. *INform 27*. Available in http://www.irca.org/en-gb/resources/INform/archive/issue27/Features/Building-on-safety21/.

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management, 46*(5), 267–270.

Star, S. L., & Ruhleder, K. (1996). Steps toward an ecology of infrastructure: Design and access for large information spaces. *Information systems research, 7*(1), 111–134.

Tikanmäki, I., Rajamäki, J., & Pirinen, R. (2014). *Mobile object bus interaction—Designing future emergency vehicles*. Vantaa: Laurea.

US Code Title 44. (2008). Chapter 35, Subchapter III, Section 35422.

Chapter 13
An Analysis of the Nature of Spam as Cybercrime

Mamoun Alazab and Roderic Broadhurst

Abstract The continued rapid growth of the Internet and the emergence of the Internet of Things (IoT) have resulted in the increased sophistication of malicious software or crime-ware tools and the refinement of deceptive methods to conduct computer attacks and intrusions. Cyber attacks via spam emails (unsolicited bulk messages) remain one of the major vectors for the dissemination of malware and many predicate forms of cybercrime. Monitoring spam as potential cybercrime can help prevention by observing changes in attack methods including the type of malicious code and the presence of criminal networks. In this paper, we describe the nature and trends in spam borne malware. This paper outlines some of the issues and problems in respect to the spam in cybercrime and gives examples of known cases and offers insight to tackle spam problems.

Acronyms

AFP	Australian Federal Police
C&C	Command and control server
CAN-SPAM	Controlling the Assault of Non-Solicited Pornography and Marketing
CoE	Council of Europe
DDoS	Distributed Denial of Service
ECPA	Electronic Communications Privacy Act
IoT	Internet of things
ISP	Internet service provider
ITU	International Telecommunication Union
Malware	Malicious software
NSW	New South Wales

M. Alazab (✉)
Macquarie University, Sydney, NSW, Australia
e-mail: mamoun.alazab@mq.edu.au

R. Broadhurst
Australian National University, Canberra, ACT, Australia
e-mail: roderic.broadhurst@anu.edu.au

R.M. Clark and S. Hakim (eds.), *Cyber-Physical Security*,
Protecting Critical Infrastructure 3, DOI 10.1007/978-3-319-32824-9_13

OECD	Organization for Economic Cooperation and Development
P2P	Peer-to-peer
PPI	Pay per install
RTA	Remote access trojan
Tor	The onion router
URL	Uniform resource locator
VPN	Virtual private network

13.1 Introduction

Cisco predicts there will be 25 billion devices connected to the Internet by 2015 and 50 billion by 2020 (Cisco 2011), creating via convergence and connectivity the Internet of Things (IoT) or the "Internet of Everything" (Cisco 2013). This represents a major transformation that has the potential to affect everyone with the growing use of mobile devices, cloud computing, and a network of networks. As Chris Young, SVP-Security Business Group at Cisco observes (Young 2014) "Each connection in the IoT brings new risks that challenge defenders to provide enhanced levels of protection. This requires a threat-centric approach to security, with solutions that work together, collecting and sharing intelligence, with a coordinated focus on threats. This is the only way to protect what matters most. With the IoTs every company becomes a technology company, and every company becomes a security company." No doubt, the Internet is one of the most important creations in human history and the use of the Internet for the purpose of crime is a rapidly growing phenomenon that requires a proactive and coordinated response (UNODC 2013). Cybercrime threatens the IoT, because of the use of increasingly sophisticated crime-ware tools and methods to distribute a wide range of malicious content combined with more difficult to detect '*social engineering*' deceptions, Spam emails, and cloaked phishing sites blend with malware tools to enhance the ease of identity theft (Smith and Hutchings 2014). Spam as a cybercrime, the focus of this paper, takes many forms and many varieties have been described in a European Commission study (European Commission 2009). Spam can merely carry annoying but benign advertising; however, they can also be the initial contact point for cybercriminals, such as the operators of a fraudulent scheme, to contact and solicit prospective victims (as in advance fee frauds), or to commit identity theft by deceiving recipients of such mail into disclosing personal, bank and financial account information (Grabosky and Smith 1998; Smith et al. 2004).

Spam remains a major vector for the dissemination but unlike 'low volume-high value' cybercrime that targets banks and financial services and requires advanced hacking capability, spam enables malware to reach 'high volume-low value' targets that are less likely to have effective antivirus or other countermeasures in place. Such malware is distributed through two types of spam: those with an attachment that contains a virus or Trojan that installs itself in the victim's computer when the

attachment is opened; and those with a hyperlink to a web page where the malware is downloaded onto the compromised computer (Alazab and Venkatraman 2013). The challenge for modern enterprises engaged in e-commerce or e-government is about how to cultivate and keep trust with customers and users as Microsoft's Scott Charney (2014) observes:

> In the world of cloud services and big data, people expect that companies will be responsible stewards of that data. Indeed, having trust in a provider will ultimately determine if people are willing to use connected products and services. Because of this, companies must be transparent about how they handle data, ensure they have robust corporate programs to protect privacy and ultimately be accountable for their actions.

13.2 Mega Spam

Unsolicited bulk emails or 'spam' pose a global challenge because of their enormous volume and they offer a simple way for disseminating malicious crimeware capable of compromising a victims' computer (Alazab 2015). Also, beside its potentially criminogenic nature, spam is problematic because of its sheer volume, which impedes the flow of legitimate Internet traffic around the world. Google enterprise security has estimated in 2009 that spam may account for 94 % of emails (The New York Times 2009), according to the International Telecommunication Union (ITU) data spam accounted for more than 80% of the total global email traffic (ITU 2014). Estimates have subsequently been lowered to an average of 66.3 % of all emails sent in the first quarter of 2014 and 68.6% in the second quarter of 2014 (Kaspersky 2014a, b). Of all emails sent on any one day, an average of 3.3 % contained malicious attachments (Kaspersky 2013). Yet, even if this proportion seems small, based on Radicati's forecast that in 2013, approximately 183 billion emails will be sent and received per day, the number of illicit and potentially malicious mails would be substantial (Radicati and Levenstein 2013). Symantec reported that worldwide 30 billion spam emails were sent each day in 2012 (Symantec 2013), 29 billion in 2013, and 28 billion in 2014 (Symantec 2015). The costs of spam are high. Rao and Reiley (2012) estimated that spammers earn gross global revenues of the order of US$200 million per year, while some US $20 billion is spent fending off unwanted emails.

13.3 Trends in Spam

While some basic elements of the early spam attacks are still apparent, much has changed during the decade since Australia's first email phishing attack in 2003 on the Commonwealth Bank. As crime follows opportunity, the various forms of Spam continually adapt and easily blend with new methods as with as in the example of blended '*ransom-ware*' attacks that use crypto-loggers). The three main trends that have become apparent in spam emails include:

- sophistication (larger spam botnets, easier to use, and increasingly automated);
- commercialization (spam botnets for rent, markets for active email addresses); and
- changing organizational forms such as diverse offender groups communicating and collaborating with each other (Grabosky 2013).

The widespread uses of botnets show how spammers manipulate the networks of infected computers and servers around the world to ensure high volumes of spam are delivered.

Spam designed to create botnets also showed increased complexity in the type of malware deployed and are designed to exploit new opportunities arising from the development of automated financial activities (e.g. *GameOver ZeuS* and *Crypto Lock*er). The Internet has also become the preferred platform to deploy spam attacks to intentionally disrupt, or to subvert these automated services and also to launch distributed denial of service (DDoS) attacks (for profit or ideological motives) (Broadhurst and Chang 2013). These tools have far reaching implications for the evolution of cyber crime, by facilitating the deployment of malware for entry level players.

13.4 The Organizational Structure of Spam as Cybercrime

The stereotypical thrill-seeking, computer-savvy cyber criminals of the 1970s and 1980s who promoted an anarchist culture of a 'free' Internet (Cao and Lu 2011) have been supplanted in the recent years by cyber criminals who apply their skills to acquire money. The transition to increasingly organized forms of cyber crime is reminiscent of a generational change; the hackers of the 1970s and 1980s tended to act alone and were often motivated by nonprofit goals, while now skilled IT criminals specialize and hire out their skills to criminal organizations. McGuire (2012) estimated that about 80% of cyber crime could be the result of some form of organized crime activity. This does not mean, however, that these groups take the form of traditional, hierarchical organized crime groups or that they commit exclusively digital crime, (Broadhurst et al. 2014). To show the increased level of organization, we describe a few examples of cyber crime committed by individuals and by crime groups or organizations. Chabinsky (2010) outlined the various 'professional positions' encountered by the FBI when investigating persistent cyber criminal enterprises. He described the most common roles and functions required to sustain systematic profit through online theft, extortion, and fraud:

1. **Programmers** who develop the exploits and malware used to commit crime.
2. **Distributors** who trade and sell stolen data and act as vouchers for the goods provided by other specialists.

3. **Technical experts** who maintain the criminal enterprise's IT infrastructure, including servers, encryption, databases, etc.
4. **Hackers** who search for and exploit applications, systems, and network vulnerabilities.
5. **Fraudsters** who create and deploy various social engineering schemes, such as phishing and spam.
6. **Hosted providers** who offer safe hosting of illicit content servers and sites.
7. **Cashiers** who control drop accounts and provide names and accounts to other criminals for a fee.
8. **Money mules** that undertake wire transfers between bank accounts. The money mules are often students who travel to the US to open bank accounts. [Mules are often recruited via spam offering 'jobs' or work that promises a relatively high commission, i.e., 3 and 5 % of the total money laundered see (Panda Security 2010)].
9. **Tellers** who are charged with transferring and laundering illicitly gained proceeds through digital currency services and different world currencies.
10. **Organization Leaders** are often 'people persons' without technical skills. The leaders assemble the team and choose the targets.

13.4.1 Examples

13.4.1.1 Individuals—Kings of Spam

James Ancheta a resident of California was a member of a loose network or group called the Botmaster Underground. In May 2006, he was sentenced to almost five years in federal prison for using his botnet to control almost half a million computers and then selling or renting access to them for $200–$300 per hour for the purpose of launching DDOS attacks and sending spam (United States District Court 2005).

Working alone, Robert Alan Soloway (aka Spam King), was one of the most persistent professional spammers, and Spamhaus had included him on its list of the 10 worst spammers. In the mid-2007, he was indicted by a grand jury in Seattle, for violation of the Computer Abuse and Fraud Act of 1984, and the 2003 CAN-SPAM Act (Controlling the Assault of Non-Solicited Pornography and Marketing) for using his extensive network of compromised computers of over four years to send tens of millions of unsolicited emails (The Washington Post 2007). Alan Ralsky was also known for his activities as a spammer and was sentenced by a federal court in Detroit in 2009 to almost five years in prison for spam, email fraud, and violations of the US CAN-SPAM Act. Ralsky sent 70 million messages a day from fake email addresses (Department of Justice 2009).

Edward "Eddie" Davidson aka 'Fast Eddie' and the 'Spam King', another notorious American email spammer sentenced by the US District Court to serve four

years in federal prison for sending hundreds of thousands of spam emails in April 2008. Prosecutors found Davidson's bank deposits from 2003-2006 amounted to $3.5 million, and that he hid $380,000 in a girlfriend's bank account and purchased gold, platinum, palladium, and silver coins worth $418,000 (Greenemeier 2008).

Oleg Nikolaenko a male 28-year-old Russian national also known as: 'Docent', and the 'King of Spam', who is believed to be behind a third of all spam in circulation. In November 2010, he was arrested when he visited a car show in Las Vegas (Krebs 2011). The US Justice Department claims that Nikolaenko earned millions of dollars using his 'Mega-D' botnet. Federal investigators believe the botnet may have been responsible for one-third of the world's electronic spam in 2009. The 'Mega-D' botnet may have infected more than half a million computers and sent over 10 billion spam email a day all under the guise of falsified header information (FBI 2010). The US Justice Department claimed that Nikolaenko also sent spam on behalf of Lance Atkinson, a New Zealand citizen resident in Australia, and other members of 'Affking', an affiliate program that marketed fly-by-night online pharmacies and knockoff designer goods. In February 2013, Oleg Nikolaenko was sentenced by the US federal court to time served plus three years' probation for violating the 2003 CAN-SPAM Act (Vielmetti 2013).

13.4.1.2 Crime Groups or Organizations

E.G.1: Commonwealth Bank

On Monday 17 March 2003, an email was sent claiming to be from "admins at Commonwealth Bank." The email asked customers to 'reactivate' their account by logging in after a technology update. But the website provided for customers to log onto, while similar to the bank's website and including its security advice, was bogus. It directed customers to a Florida hosted copy of the Commonwealth Bank of Australia website. Australian Federal Police (AFP) and NSW Police started an investigation that focused on tracing the flow of funds from victims to the unknown offenders. The money was transferred to the account of a Tasmanian man who had been recruited by a Croatian Community website to receive the money and then transfer it to Eastern Europe. The AFP arrested him when he tried to draw some of the fraudulently obtained funds out of his own account but he escaped prosecution at the time as he claimed he was unaware that the money was illegally obtained (McCombie et al. 2009).

E.G.2: GameOver ZeuS

The *GameOver* ZeuS toolkit was apparently controlled and maintained by a core group of hackers from Russia and Ukraine, since October 2011. *GameOver* is based on code from the wellknown ZeuS Trojan. Computers infected with *GameOver* were used to collect sensitive information and to disseminate spam and phishing

messages. In May 2014, the US Justice Department alleged the author of the ZeuS Trojan was Evgeniy Mikhailovich Bogachev of Anapa, Russian Federation, aka "Slavik," and "Pollingsoon." In June 2014, a multinational effort designated *Operation Tovar* was necessary to disrupt the *GameOver* ZeuS Botnet. The FBI, UK National Crime Agency, and Europol/EC3, as well as industry based information security providers were involved. Target computers were hacked when the victims opened a seemingly harmless email. This enabled access to the computer's data such as bank account numbers and password details. Cyber criminals in Ukraine were then able to log on to the stolen bank accounts and illegally withdraw funds. Associates of the Ukrainian organizers advertised on Russian language websites inviting students living in the US to help in transferring the stolen funds out of the country. These 'mules' were provided with fake passports and asked to open accounts under false names in various US banks, building societies, and other financial institutions. Ukraine-based organizers transferred funds from the victims' legitimate accounts to their mules' accounts, who were then instructed to transfer the money to offshore accounts or to physically smuggle it out of the US. Five persons were arrested in Ukraine, 11 in the United Kingdom, and 27 in the US (8 more were charged by US authorities but remain fugitives). (The U.S. Justice Department 2014).

13.5 Spam Botnets

Spam thrives on the acquisition of active email addresses and these addresses are harvested in three different ways; first, by searching for email addresses listed on web sites and message boards; second, by performing a 'dictionary attack', a combination of randomly generated usernames with known domain names to guess correct addresses; and finally, by purchasing address lists from other individuals or organizations such as in underground markets (Takahashi et al. 2010). In 2012, Trend Micro reported that more than half of the total number of spam email addresses collected from February to September 2012 were obtainable from web sites alone (Trend Micro 2012). Once email addresses are harvested, spammers distribute spam by using botnets. This technique is essential for large spam botnets, often identified by their illicit marker brands such as Storm Worm, Grum, Mega-D. Bobax, Cutwail, Maazben, Rustock, and others. These botnets operate as bulk mailers or open-relays and hide the real address of the spammer (Stringhini et al. 2011).

The uses of botnets show how spammers have learned to manipulate the networks of compromised computers and servers around the world to ensure how high volumes of spam are delivered. Botnets require a command and control (C&C) server to coordinate targets and evade blacklisting services and this is the target for anti-spam investigations by public and private actors. Botnet-based spam may have emerged around 2004 as a type of novel advanced distribution network

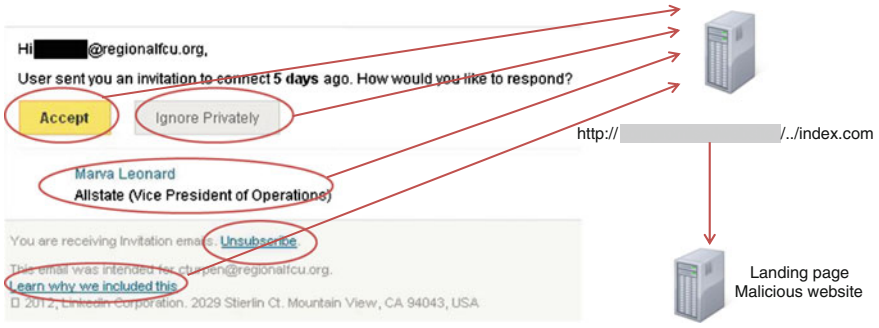


Fig. 13.1 Example of redirect link 'waterhole' attacks

(also associated with DDoS attacks) and responsible for almost all large-scale spam campaigns. Fully automated spam campaigns often include malicious spam created by crime-ware toolkits, such as Black hole, that can insert via malicious URLs or malicious attachments advanced intrusion software.

Spam often contains a malicious attachment or a link to legitimate web sites that have been compromised by a web attack toolkit. These toolkits are easy to use and efficiently leverage existing vulnerabilities. For instance, the well-known Black hole attack toolkit has been applied in some spam campaigns. A recent criminal innovation involves attacking computers indirectly by concealing intrusions through an intermediary website or 'waterhole', i.e., sites that the target is likely to visit, and that also host malicious code on the landing page (see Fig. 13.1). Cybercriminals also create links in spam messages that point to exploit portals hosting Black hole, an alternative approach that avoids the need to hack legitimate websites before planting malicious code.

Automation occurs, using a template-format for spam content distributed through thousands of compromised computer hosts (or 'zombies') available to a botmaster who charges fees to do so. A 2010 McAfee Threat Report (McAfee 2010) stated that most spam traffic comes from compromised computers. Consequently spam driven malicious attacks, often amplified by botnet applications, have become more organized and targeted. Compromised computers are infected with software bots that allow the computers to be controlled remotely through an established C&C. The analysis shows that 40% of our dataset consist of emails that have been distributed more than 50 times and sometimes more than 1000 times (either with the same or different attachments), suggesting that these spam emails have been sent by different groups, using botnets to distribute them.

Under the control of C&C servers, botnets become powerful and effective 'slave' computing assets that can be rented for illegal activities such as sending malicious spam. The malware once installed is then used to steal sensitive information (to be sold or used later), and the infected computer used to send spam, or install other malicious codes (e.g. fake anti-virus services).

13.6 Spammers and Underground Forums

For this account, some typical discussion forum threads monitored by our colleague Steve Chon from both open and closed sources were selected to illustrate how these different facets of preparation converge. The first discussion involves encryption for a Remote Access Trojan (RAT) or a bundled Remote Administrator Tool, mostly used for malicious purposes, such as controlling computers, and stealing data. RATs often spread over P2P file sharing programs (such as uTorrent, Pirate Bay etc.) and/or Messengers (such as MSN, Skype, Yahoo, AIM etc.) and email spams. Examples from a larger study in progress on underground discussion forums focusing on crime-ware toolkits are shown in Box 13.1.

Box 13.1: Examples of discussion forum threads

Discussion 1: **Crypter for RAT's**:

"So I am using DarkComet and it's awesome, but I need a crypter so it will crypt everything in a exe file so that antivirus doesn't detect it. Thanks for the help, my friend and I have looked everywhere for a good free one but have had no luck."

Discussion 2: **Not wanting to use ZeuS or SpyEye**:

"Already have my own crypter and rat set up with slaves (botnet). Can reverse proxy them to get around a number of issues. The next step I suppose is to invest in a good form grabber. Hard to find on the open net and HackBB doesn't have a lot of programming vendors. Got any suggestions?"

Discussion 3: **BlackShades NET V2.2 Cracked**:

"Deciding between a RAT, a host booter, or controlling a botnet has never been easier. With Blackshades NET, you get the best of all three - all in one with an easy to use, nice looking interface. You are able to choose between four crisp looking skins, with the default being a very nicely-fitting black theme. Even better, Blackshades NET does a lot of the work for you - it can automatically map your ports, seed your torrent for you, and spread through AIM, MSN, ICQ and USB devices."

Discussion 4: **"[Tutorial] Epic RAT Spreading Guide| Detailed Methods"**

"In the last time i saw a lot of people asking for help with spreading there keylogger or there RAT. Now i decided to make a huge tutorial on spreading to help the community. I will start with very basic and famous stuff like youtube and also a few advanced methods. General Things you need:

a RAT (ready set-up, make sure its working)
a crypter (you will get a lot more victims if your server is FUD)
a filehost (for example fileave or dropbox)
a computer
a brain would not be bad; D…"

In these examples, a crypter and an unnamed RAT had been used to create a botnet. But the discussant is also seeking a 'form grabber' typically found in banking RATs such as ZeuS. A 'form grabber' is a tool that steals data entered into a web browser by a victim.

There were also examples of multiple crime-ware tools being distributed. In one example, both a ZeuS and a crypter were offered together, in addition to "Ice9" a variant of ZeuS. In another example, a version of BlackShades were posted for download and offered 'all in one' features such as a RAT, host booter (applied in a DDoS attack), and a botnet C&C.

Thus, a range of crime-ware tools were used in combination for the purpose of creating botnets—suitable for spam mass distribution or targeted intrusions. In the last example, a method to spread RATs or keyloggers, compromising many computers and to create a botnet is discussed.

Figure 13.2 shows a screenshot of a fake PayPal email that illustrates an exploit kit (Blackhole) and a RAT being used for the purpose of creating a botnet and delivered via a spam message—part of a spam campaign. This is a typical example of social engineering (Chantler and Broadhurst 2006). Although the email appears

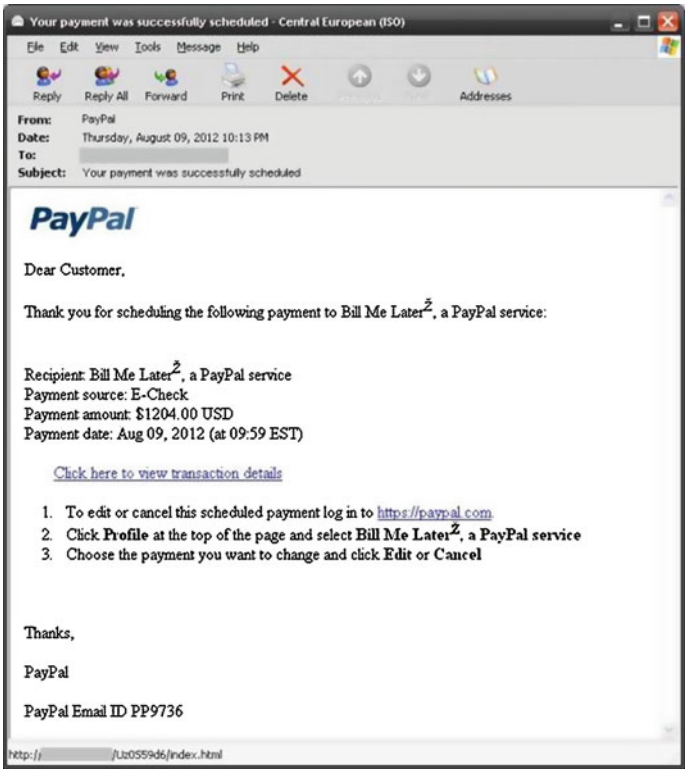


Fig. 13.2 A spam email including a blackhole exploit

to be legitimate, it contains a malicious URL, which when clicked upon redirects the victim's computer, through a number of websites unseen to the victim, to a website that contains the Black hole exploit kit.

13.7 Countermeasures

Technological or legal responses alone are not as effective as those that combine technical methods with sound law enforcement and crime prevention practices and process. Many victims are simply deceived by clever methods (often mimicking trusted sources) and are often over confident about their ability to detect spam. Coordinated operations by police and private cyber security providers are needed to takedown several complex spam/malware botnets (e.g. McColo, GameOver ZeuS, Grum, Coreflood, Rustock). The advantage of legal processes. The benefits of international police and private industry cooperation is that they readily mandate the removal of all the top-level domain names associated with spam even though the investigations cannot remove the techniques used or arrest the offenders involved. The efforts to disrupt the *GameOver ZeuS* botnet illustrates the need for common mutual legal assistance across borders and the role of private sector security firms and NGOs including CrowdStrike, Dell SecureWorks, Symantec, Trend Micro, McAfee; and academic researchers at VU University Amsterdam and Saarland University in Germany. These combined law enforcement responses to complex cybercrime activities, thus depend on the role of private information security businesses to achieve the most effective solution (OECD 2006; Krebs 2014).

Some laws, regulations, and policies, however, can sometimes hinder the effectiveness of public or private actions. Policies such as "Network (Net) Neutrality" or common carrier policies (European Commission 2009; Darrell 2009) can hinder Internet Services Providers (ISPs) and other network providers from acting to eliminate criminal traffic from their networks because of the risk of breaching network neutrality regimes. Even in states where laws do not specifically preclude action, the conventional approach is to minimize possible interventions by ISPs and other actors that could counter or eliminate undesirable behavior (e.g. hate mail, spamming etc.). A potential response would be to reframe network neutrality laws or practices to allow for the redirection of Internet traffic flows when such traffic indicate a high risk of being malicious. Under some interpretations of privacy laws such as the United States' Electronic Communications Privacy Act (ECPA), companies that detect illegal activity on their networks are unable voluntarily to share information about such activities with other parties (e.g. other ISPs, information security firms) in order to prevent further illegal activity. For instance, corporations are concerned about sharing nonredacted spam and phishing mail feeds, for fear of unintentionally violating their customers' privacy rights under the ECPA (Barrett et al. 2011). Similar concerns prevail in Australia and other jurisdictions and have the effect of fragmenting collective countermeasures and create barriers to applied research on such problems.

Email spam filtering, from a computer science prospective, is a mature research field with many filtering techniques available such as rule, information retrieval, and graph based, as well as machine learning and hybrid techniques. However, identifying emails with malicious content remains a problem worthy of further investigation (Tran et al. 2013; Alazab et al. 2013). One recent study of spam and phishing identified the location of high risk ISPs that acted as "Internet bad neighbours," and found that spam originates from a small number of ISPs. The majority of "bad" ISPs were concentrated in India, Brazil, West Africa, and Vietnam. For example, 62% of all the addresses serviced by Spectranet, an ISP in Nigeria, were sending out spam (Moura 2013). In 2009, the US Federal Trade Commission for example closed down the ISP 3FN Service, as it was found to be hosting spam-spewing botnets, phishing websites, child pornography, and malicious web content (Federal Trade Commission 2009). However, Trend Micro reported that it was back in business a few days after—reinvented but established outside US jurisdiction (Trend Micro 2010).

National and international agencies, the United Nations, Interpol, The International Telecommunications Union European Union, Council of Europe (CoE), Organization for Economic Cooperation and Development (OECD), and other regional and regulatory agencies have all strived to create a seamless web of international law to address cybercrime but as yet universal coverage has not been achieved. The CoE's Cybercrime Convention known as the 'Budapest Convention' 2001; effective 2004 provides a comprehensive international approach to cybercrime investigation and a model law that enhances harmony across the laws of different jurisdictions. The convention formalizes mutual legal assistance arrangements between jurisdictions and includes several non-European states such as the USA, Japan, Australia, Canada, and South Africa but critically not Russia, China, Brazil, Nigeria, and India. However, the Convention drafted in 1999, despite efforts to account for rapid technological change, has not kept pace with innovations such as botnets. This lack of universality and currency of laws to suppress cybercrime combined with the absence of effective law enforcement in many countries renders cross-jurisdictional investigations often ineffective (Broadhurst 2006). Shifts to cloud-based computing has also unsettled well-practiced firewall security measures and cloud services are often less visible to company IT security. However, cross-border cooperative efforts such as the London Action Plan on SPAM, which bring willing actors both state and non-state are the key to improved counter measures.

Several factors are crucial in countering the impact of spam fed cybercrime and remain highly problematic for organizations forced by the convergence in communications and the need to be cybersecure. Among the most pressing are the need to establish effective public and private partnerships, like the London Action Plan and *Signal-Spam,*[1] to make cross jurisdiction, and cross-culture cooperation

[1]Signal-Spam was initiated in 2005 as a public–private organization to identify spammers for enforcement cases.

work, and to train more skilled cybercrime investigators and information security specialists. Improved means of tracking and identifying offenders are also needed and such efforts need to manage the cross-border legal barriers that effectively hinder rapid responses by law enforcement in terms of data seizure and preservation (Blackstone and Hakim 2013). Improving Public–Private Partnerships is thus essential in reducing the risks for Internet users. An early example was the cooperation between the FBI, Moroccan authorities, Ministry of Interior Turkish National Police, and Microsoft lead to the arrests of Farid Essebar, a Moroccan national and Atilla Ekici, aka "Coder" of distributors of the "Mytob" and "Zotob" computer Virus (FBI National Press Office 2005).

Another threat is the rapid growth of underground markets, trading forums, and Instant Messaging sites, which can be a source of profit for many cybercriminals. These services reduce the barriers for new actors to engage in cybercrime and are offered by online crime groups that provide illicit services such as renting or creating botnets, databases with email addresses and attack services. Hackers and organized crime groups operate with little hindrance in these illicit markets hidden in encrypted Virtual private networks (VPNs) such The Onion Router[2] (TOR) like settings often selling confidential stolen data or facilitating their theft. When combined with the widespread use of ready to use 'toolkits' deep web 'dark-markets' have greatly amplified the impact of cybercrime. Toolkits enable even a novice to undertake a cybercrime and they can start easily by contributing to pay per install (PPI) services that have also developed into an underground criminal industry. Disrupting these 'dark-net' markets is time consuming and often temporary. In such a climate, enterprises operating in the e-commerce or e-government environment are compelled to invest significantly in the protection of their databases (client details etc.) and must acquire the technical and security awareness to counter the persistent cyberthreats now faced.

References

Alazab, M. (2015). Profiling and classifying the behavior of malicious codes. *Journal of Systems and Software, 100*, 91–102. doi:10.1016/j.jss.2014.10.031.

Alazab, M., Layton, R., Broadhurst, R., & Bouhours, B. (2013, November 21–22). *Malicious Spam Emails Developments and Authorship Attribution, IEEE.* Paper presented at the The Fourth Cybercrime and Trustworthy Computing Workshop, Sydney NSW.

Alazab, M., & Venkatraman, S. (2013). Detecting malicious behaviour using supervised learning algorithms of the function calls. *International Journal of Electronic Security and Digital Forensics, 5*(2), 90–109.

[2]Tor is free software and an open network that helps internet users defend against network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security.

Barrett, M., Steingruebl, A., & Smith, B. (2011). Combating cybercrime: Principles, policies, and programs, from https://www.paypal-media.com/assets/pdf/fact_sheet/PayPal_CombatingCybercrime_WP_0411_v4.pdf

Blackstone, E. A., & Hakim, S. (2013). Competition versus monopoly in the provision of police. *Security Journal, 26*, 157–179.

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies and Management, 29*(3), 408–433.

Broadhurst, R., & Chang, L. (2013). Cybercrime in Asia: Trends and challenges. In J. Liu, B. Hebenton & S. Jou (Eds.), *Handbook of Asian criminology* (pp. 49–63). New York: Springer.

Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2014). Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime. *International Journal of Cyber Criminology, 8*(1), 1–20.

Cao, X., & Lu, Y. (2011). Social network analysis of a criminal hacker community. In H. Nemati (Ed.), *Security and privacy assurance in advancing technologies: New developments* (pp. 160–173). IGI Global.

Chabinsky, S. (2010). *The cyber threat: Who's doing what to whom?* Paper presented at the GovSec/FOSE conference, Washington, D.C. http://www.fbi.gov/news/speeches/the-cyber-threat-whos-doing-what-to-whom

Chantler, A., & Broadhurst, R. (2006). *Social engineering and crime prevention in cyberspace*. Technical Report, Justice, Queensland University of Technology, from http://eprints.qut.edu.au/7526/1/7526.pdf

Charney, S. (2014). An atlas of internet insecurity. Retrieved November 7, 2014 from http://forbesindia.com/printcontent/38270

Cisco. (2011). The internet of things how the next evolution of the internet is changing everything, Cisco Internet Business Solutions Group (IBSG). Retrieved June 5, 2015 from http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

Cisco. (2013). The internet of everything for cities: connecting people, process, data, and things to improve the 'livability' of cities and communities. Retrieved November 20, 2015 from http://www.cisco.com/web/about/ac79/docs/ps/motm/IoE-Smart-City_PoV.pdf

Darrell, K. (2009). *Issues in internet law: Society, technology, and the law*. Amber Book Company.

Department of Justice. (2009). Detroit spammer and three co-conspirators sentenced for multi-million dollar e-mail stock fraud scheme, from http://www.justice.gov/opa/pr/2009/November/09-crm-1275.html

European Commission. (2009). EU study on the legal analysis of a single market for the information society: New rules for a new age? from http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=7022&

FBI. (2010). Russian man charged with sending thousands of spam e-mails from http://www.fbi.gov/milwaukee/press-releases/2010/mw120210a.htm

FBI National Press Office. (2005). FBI announces two arrests in Mytom and Zotob computer worm investigation. Retrieved October 13, 2014 from https://www.fbi.gov/news/pressrel/press-releases/fbi-announces-two-arrests-in-mytob-and-zotob-computer-worm-investigation

Federal Trade Commission. (2009). FTC shuts down notorious rogue internet service provider, 3FN service specializes in hosting spam-spewing botnets, phishing web sites, child pornography, and other illegal, malicious web content, from http://www.ftc.gov/news-events/press-releases/2009/06/ftc-shuts-down-notorious-rogue-internet-service-provider-3fn

Grabosky, P. (2013). Organised crime and the internet. *The Royal United Services Institute (RUSI) Journal, 158*(5), 18–25. doi:10.1080/03071847.2013.847707

Grabosky, P., & Smith, R. (1998). *Crime in the digital age: Controlling telecommunications and cyberspace illegalities*. Piscataway: Transaction Publishers.

Greenemeier, L. (2008). A tale of two "Spam Kings" from http://www.scientificamerican.com/article/a-tale-of-two-spam-kings/

ITU. (2014). ITU and internet society collaborate to combat spam, May 2, from http://www.itu.int/net/pressoffice/press_releases/2014/61.aspx#.VpRYVRV96Uk

Kaspersky. (2013). Spam in Q1 2013. Retrieved August 8, 2015 from https://securelist.com/analysis/quarterly-spam-reports/36497/spam-in-q1-2013/

Kaspersky. (2014a). Spam and phishing in Q2 2014. Retrieved December 8, 2014 from https://cdn.securelist.com/files/2014/08/Spam-report_Q2-2014_en.pdf

Kaspersky. (2014b). Spam and phishing statistics report Q1-2014. Retrieved October 1, 2014 from http://usa.kaspersky.com/internet-security-center/threats/spam-statistics-report-q1-2014#.VpRChhV96M8

Krebs, B. (2011). Chats with accused 'Mega-D' botnet owner? from http://krebsonsecurity.com/2011/12/chats-with-accused-mega-d-botnet-owner/

Krebs, B. (2014). Operation Tovar' targets 'Gameover' ZeuS botnet, cryptolocker scourge, from http://krebsonsecurity.com/2014/06/operation-tovar-targets-gameover-zeus-botnet-cryptolocker-scourge/

McAfee. (2010). McAfee threats report: Second quarter 2010, from http://www.redteamusa.com/PDF/McAfee/McAfee_Labs_Threat_Report_2nd_quarter_2010.pdf

McCombie, S., Pieprzyk, J., & Watters, P. (2009). *Cybercrime attribution: An eastern european case study*. Paper presented at the 7th Australian digital forensics conference, Perth, Western Australia.

McGuire, M. (2012). *Organised crime in the digital age*. London: John Grieve Centre for Policing and Community Safety.

Moura, G. (2013). Internet bad neighbourhoods, University of Twente, Doctor degree, from http://doc.utwente.nl/84507/1/thesis_G_Moura.pdf

OECD. (2006). OECD anti-spam toolkit of recommended policies and measures. Retrieved August 4, 2014 from http://www.oecd.org/internet/consumer/36494147.pdf

Panda Security. (2010). Panda security report: The cyber-crime black market: Uncovered from http://press.pandasecurity.com/wp-content/uploads/2011/01/The-Cyber-Crime-Black-Market.pdf

Radicati, S., & Levenstein, J. (2013). Email statistics report, 2013–2017, from http://www.radicati.com/wp/wp-content/uploads/2013/04/Email-Statistics-Report-2013-2017-Executive-Summary.pdf

Rao, J., & Reiley, D. (2012). The economics of spam. *Journal of Economic Perspectives, 26*(3), 87–110. doi:10.1257/jep.26.3.87.

Smith, R., Grabosky, P., & Urbas, G. (2004). *Cyber criminals on trial*. Cambridge: Cambridge University Press.

Smith, R., & Hutchings, A. (2014). *Identity crime and misuse in Australia: Results of the 2013 online survey*. AIC Reports Research and Public Policy Series, from http://aic.gov.au/media_library/publications/rpp/128/rpp128.pdf

Stringhini, G., Holz, T., Stone-Gross, B., Kruegel, C., & Vigna, G. (2011, August 8–12). *BOTMAGNIFIER: Locating spambots on the internet*. Paper presented at the 20th USENIX conference on security, San Francisco, CA.

Symantec. (2013). Internet security threat report 2013: Volume 18, from https://scm.symantec.com/resources/istr18_en.pdf

Symantec. (2015). Internet security threat report. Retrieved December 2, 2015 from https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347931_GA-internet-security-threat-report-volume-20-2015-appendices.pdf

Takahashi, K., Sakai, A., & Sakurai, K. (2010). Spam mail blocking in mailing lists. In K. Nishi (Ed.), *Multimedia*. InTech.

The New York Times. (2009). Spam back to 94 % of all e-mail. Retrieved September 12, 2013 from http://bits.blogs.nytimes.com/2009/03/31/spam-back-to-94-of-all-e-mail/?_r=0

The U.S. Justice Department. (2014). A complaint USA v Evgeniy Bogachev, from http://www.justice.gov/opa/documents/dgzc/complaint.pdf

The Washington Post. (2007). Longtime 'Spam King' charged with fraud. Retrieved September 7, 2013 from http://www.washingtonpost.com/wp-dyn/content/article/2007/05/31/AR2007053100310.html

Tran, K.-N., Alazab, M., & Broadhurst, R. (2013). *Towards a feature rich model for predicting spam emails containing malicious attachments and urls.* Paper presented at the Eleventh Australasian Data Mining Conference Canberra, ACT.

Trend Micro. (2010). *The botnet chronicles: A journey to infamy*. A trend micro white paper, from http://countermeasures.trendmicro.eu/wp-content/uploads/2012/02/the_botnet_chronicles_-_a_journey_to_infamy__nov_2010_.pdf

Trend Micro. (2012). Spear-phishing email: Most favored APT attack bait, from http://www.trendmicro.com.au/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf

United States District Court. (2005). United States District Court for the Central District of California: US vs Jeanson Ancheta, Case order 05-1060, from http://news.findlaw.com/hdocs/docs/cyberlaw/usanchetaind.pdf

UNODC. (2013). Comprehensive study on cybercrime, from http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Vielmetti, B. (2013). Russian king of spam avoids prison in plea deal. Retrieved October 23, 2014 from http://www.jsonline.com/blogs/news/195458101.html

Young, C. (2014). An atlas of internet insecurity. Retrieved November 7, 2014 from http://forbesindia.com/printcontent/38270

Chapter 14
Securing the Automotive Critical Infrastructure

Dennis Kengo Oka

Abstract As increasingly more vehicles are becoming interconnected and interact with their surroundings, i.e., the emergence of the *connected car*, we see a greater need for cyber security solutions applied within the automotive industry and transportation systems. Since millions of vehicles and potentially human lives could be affected, the connected car scenario can be seen as a critical infrastructure where both security and safety are equally paramount. It is imperative to consider appropriate cyber security solutions, and especially take into consideration solutions that will fulfill automotive requirements in terms of safety, performance and cost. This chapter explores automotive security advancements such as automotive-grade hardware security modules, secure vehicle-to-X (V2X, i.e., vehicle-to-vehicle and vehicle-to-infrastructure) communications, secure in-vehicle communications and embedded security evaluations of automotive components. Automotive hardware security based on EVITA, serves as a trust anchor where additional security solutions can be built upon. V2X communication is protected based on established industry standards to provide both authenticity and privacy. A Secure Onboard Communication module is responsible for providing secure in-vehicle network communication. For security evaluations, both theoretical evaluations and practical security testing of embedded systems are becoming increasingly important. Above security advancements provide an insight into what is necessary to protect a critical infrastructure such as transportation systems.

Acronyms

AES	Advanced Encryption Standard
AES-CMAC	Advanced Encryption Standard Cipher-based Message Authentication Code
ASIC	Application specific integrated circuit
AUTOSAR	AUTomotive Open System ARchitecture
CA	Certificate authority

D.K. Oka (✉)
ETAS K.K., Queen's Tower C-17F, 2-3-5 Minatomirai, Nishi-ku,
Yokohama 220-6217, Japan
e-mail: dennis-kengo.oka@etas.com

R.M. Clark and S. Hakim (eds.), *Cyber-Physical Security*,
Protecting Critical Infrastructure 3, DOI 10.1007/978-3-319-32824-9_14

CAN	Controller Area Network
ECU	Electronic control units
EVITA	E-safety vehicle intrusion protected applications
FTC	Federal Trade Commission
IEEE	Institute of Electrical and Electronics Engineers
MAC	Message Authentication Code
NHTSA	National Highway Traffic Safety Administration
NIST	National Institute of Standards and Technology
OBD	On-board diagnostics
OEM	Original equipment manufacturer
PKI	Public key infrastructure
PRESERVE	Preparing secure V2X communication systems
SAE	Society of Automotive Engineers
SecOC	Secure onboard communication
V2I	Vehicle-to-infrastructure
V2V	Vehicle-to-vehicle
V2X	Vehicle-to-X
WMA	Windows Media Audio

14.1 Introduction

This chapter focuses on automotive security, and describes cyber security attacks targeting vehicles and their infrastructure and also gives a presentation of appropriate solutions. In July, 2015, security researchers demonstrated that they could remotely take control of a vehicle driving on a highway and kill its engine which eventually resulted in a recall of 1.4 million vehicles (Greenberg 2015). One can imagine malicious attackers being able to exploit similar security flaws effectively crippling the vehicle fleet of an entire nation. For example, terrorist groups could with little effort remotely launch attacks that could lead to vehicle accidents as well as cause vehicles to come to a standstill affecting several other business sectors. One can also imagine such attacks on all types of transportation systems such as buses, trucks and emergency vehicles.

In recent years, the interest in automotive security has grown at an unprecedented rate. For example, within academia, there are numerous annual security conferences focusing solely on automotive security and special sessions in security conferences dedicated to automotive security. At major hacking conferences such as DEF CON and Black Hat, automotive hacking presentations have garnered vast attraction. There are also governmental movements, for example, US Senator Edward Markey issued a letter to 20 auto manufacturers in December 2013 inquiring about their security practices (Markey 2013). The letter contained questions regarding the level of security testing the auto manufacturers perform, the level of security reviews they perform and the security practices they follow. A summary of the responses was

released to the public in February 2015 (Markey 2015a). The gist is that most auto manufacturers had at the time the Markey letter was issued not considered security threats and security solutions adequately in their products but the positive takeaway is that auto manufacturers have since the Markey letter was issued already started or are planning to improve security. For example, in the past couple of years, auto manufacturers and automotive component suppliers have created dedicated security groups and employed several security engineers.

In 2015, US Senators Markey and Blumenthal introduced legislation called Security and Privacy in Your Car (SPY Car) Act (Markey 2015b). The proposed legislation sets minimum standards and transparency rules to protect the data, security and privacy of drivers of connected vehicles. The SPY Car Act includes several cyber security and privacy standards, as well as a rating system called "cyber dashboard" that informs consumers how well the vehicle protects the drivers' security and privacy (Markey 2015c). Examples of cyber security standards are: hacking protection (all access points in vehicle should be equipped with reasonable measures to protect against hacking), data security (all collected data should be secured to prevent unwanted access) and hacking mitigation (vehicle should be equipped with technology that can detect, report and stop hacking attempts). Examples of privacy standards are: transparency (making owners explicitly aware of collection and use of driving data), consumer choice (owners are able to opt out of data collection), and marketing prohibition (personal information may not be used for advertising and marketing purposes without owner agreement). The "cyber dashboard" should be established by National Highway Traffic Safety Administration (NHTSA) in consultation with Federal Trade Commission (FTC) and display an evaluation of how well the vehicle protects both the security and privacy of vehicles owners beyond the minimum standards. This information should be presented and placed on a window sticker on all new vehicles.

Combining the fact that the automotive market is a multi-billion dollar industry with advances in automotive hardware and software technologies, there are huge incentives to introduce novel business models such as over-the-air software updates, remote diagnostics and various customization offerings. However, in order to be able to offer such new services, automotive security is necessary. Moreover, cyber attacks on vehicles have also increased heavily in the past few years. The reasons for such attacks are that more systems are managed and controlled electronically (rather than for example mechanically or manually) and that more systems are interconnected. Electronic Control Units (ECUs) are small computers in a vehicle responsible for a majority of the functions in the vehicle. The number of ECUs in a vehicle is steadily increasing over the years as more advanced functions such as lane keep assist systems, automatic braking, automatic parking etc. are handled by the vehicle. Typically, modern vehicles have between 50 and 70 ECUs. As more advanced functions are supported, more complex software solutions are applied which could be targeted by an attacker. Another important reason for increased cyber attacks on vehicles is that security is often not part of the current design; safety is the number one priority and as a result security is often overlooked.

Examples of attacks that have already occurred in the field are, for example, odometer manipulation, chip tuning and theft of vehicles using the connector port for diagnostics tools. The odometer manipulation attack is something that has been ongoing for decades and has even become more prevalent in the past few years. Since modern odometers are electronic devices controlled by software rather than mechanical devices; such devices can be tampered with using special equipment. In Europe, the cost of odometer manipulation is estimated to six billion euro annually and, consequently, auto manufacturers are constantly taking measures to prevent odometer manipulation (ADAC 2014). Chip tuning is another attack that has a long history. Car owners can use chip tuning as a way to improve the performance of their engines. One concern from auto manufacturers is that if an engine would break down due to overexertion as a result of the chip tuning, an attacker could simply downgrade the software to the original version and have the engine repaired on warranty which would incur additional costs for the Original Equipment Manufacturer (OEM).

Theft of vehicles using the diagnostics connector is a relatively new attack. In 2012, it was reported that high-end cars were the target of such car thefts (Howard 2012). Typically, modern car keys are electronically encoded to ensure that they can only be used with a specific car. It was shown that an attacker who can access the On-Board Diagnostics (OBD) port on a car can connect special equipment and program a new car key specifically encoded to be used with the car to be stolen. Using the newly programmed car key enables the attacker to then drive off with the stolen car. Statistics show that the penetration of electronic theft methods varies from country to country between 0.5 and 16 % of all car thefts, however it is becoming increasingly popular in recent years. More indicative of the situation is to look at newer cars, for example, electronic theft accounts for 29 % of cars that are five years old or newer in the London area. For luxury cars or high-risk cars the figure rises to 60 % (IQPC 2012).

Within academia, more advanced and complex attacks have been successfully performed. For example in 2010–2011, researchers at University of Washington and University of California San Diego, conducted analyses of a modern vehicle and found several security issues (Koscher et al. 2010; Checkoway et al. 2011). There are two parts to their research: (1) what an attacker can do once access is provided to the internals of a vehicle and (2) how an attacker could gain remote access to the internals of a vehicle. For the first part, it is shown that an attacker can essentially take control of any ECU in the vehicle by sending the appropriate commands on the in-vehicle Controller Area Network (CAN) bus. The researchers show that it is possible to unlock the doors, enable or disable the brakes, cause the engine to fail or force the engine to not start. Consequently, it would be possible for an attacker to affect functions that would have an impact on vehicle safety. For the second part, it is shown that various external interfaces such as Bluetooth, telematics and media player exist that if exploited could allow an attacker to gain access to the internal in-vehicle network. The researchers show, for example, that by exploiting software bugs in the telematics unit, it is possible to gain remote access to the vehicle, upload new software and reprogram the gateway unit to bridge the in-vehicle networks to send commands to the target ECU (e.g., the engine ECU). Another example is crafting a specific Windows Media Audio (WMA) file that exploits a software bug in

the media player running on the infotainment system. An unsuspecting user playing a CD with the specifically crafted WMA file would result in launching an attack where the software bug in the media player is exploited causing certain commands to be injected on the in-vehicle network and sent to the target ECU.

In 2013, Miller and Valasek presented findings of a security analysis of two vehicles based on access to the in-vehicle CAN bus, e.g., by connecting directly to the OBD port (Miller and Valasek 2013). The findings included several cyber-physical attacks executed by sending messages on the in-vehicle network to kill the engine, disable the brakes or cause the steering wheel to turn. For example, an automatic parking feature on one of the vehicles they analyzed has some safety constraints such that it can be executed only when the gear is in reverse and the vehicle speed is less than 8 km/h. However, the software running on the ECU responsible for this feature receives such information from the CAN bus. The CAN bus is prone to spoofing attacks as any device connected to the CAN bus can send a message to any other device. Consequently, an attacker can falsify this information such that the automatic parking software believes that the car is in reverse and traveling slower than 8 km/h. Thus, when the gear is in drive and traveling at 120 km/h it can be tricked to believe it is in a safe condition to allow the execution of the automatic parking feature. An attacker can then trigger the automatic parking feature by sending the corresponding message on the CAN bus which would cause the steering wheel to automatically turn believing it is going to park the car; however, in actuality the car is traveling at high speeds where a sudden automatic steering wheel turn could cause an accident with devastating consequences. As more cyber-physical features that can affect the steering, braking and acceleration of vehicles are introduced, attackers can target and abuse these features to cause safety, operational and financial damage.

Miller and Valasek (2014) followed-up their research with a study of remote attack surfaces of over 20 vehicles. This study highlights where target components are located in the in-vehicle network topology, possible remote entrypoints and potential attack paths (e.g., if engine and brake ECUs are connected to the same in-vehicle network as the head unit which provides WiFi and cellular communication, an attacker could first gain entry to the head unit and from there attack the engine and brake ECUs).

In 2012, NHTSA opened a special division dedicated to automotive cyber security threats. The Electronic Systems Safety Research Division is responsible for evaluating, testing, and monitoring potential automotive cyber vulnerabilities (NHTSA 2015). With more than 60 million vehicles produced yearly since 2012, a critical vulnerability in vehicles with remote connectivity could allow cyber terrorists to target millions of vehicles in a large-scale attack to cause massive damage. Rodney Joffe, senior vice president and chief technologist at Neustar, and a small group, including Dr. Stefan Savage of the Center for Automotive Embedded Systems Security (University of California San Diego/University of Washington), executed a series of cyber-threat exercises for the Obama Administration in 2013. The Department of Homeland Security runs “Cyber Storm” exercises focusing on simulated attacks on digital infrastructure but Joffe’s exercise focused on cyber

attacks on vehicles. For example, Joffe and his group demonstrated that they were able to remotely unlock, start and drive away a vehicle from over 2000 km away. They had full control of the car's throttle, brakes and steering (AUTOWEEK 2013).

14.2 Automotive Trends

There are several technological advancements and trends within the automotive industry. For example, the notion of the *connected car* has become a commonplace where the car is becoming an even more integral part of our lives. In the past, the car was an isolated unit with network communication only over its internal in-vehicle network and typically there was no external communication interfaces. In 2015, the automotive trends are software updates over-the-air, remote diagnostics, vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications where the car is envisioned to have multiple external connections and cars themselves will be seen as nodes on larger interconnected networks.

Software in modern vehicles has grown to the size of 80–100 million lines of code and it is estimated that about 50 % of the cost to produce a vehicle in 2015 is related to electronic components. Moreover, as software is responsible for more advanced functions and thus as more complex code is developed, the risk of introducing software bugs increases. Just since 2010, millions of cars have been recalled due to software issues. *Software updates over-the-air* for the infotainment system and other in-vehicle control systems is seen as a promising solution that auto manufacturers are aiming to offer in the near future from 2015.[1] Some companies such as General Motors, BMW, Toyota and Mercedes-Benz already have software updates over-the-air capabilities for their telematics/infotainment systems. There are several advantages with software updates over-the-air: (1) it is possible to reduce the high costs associated with recalls since there is no need to actually recall any vehicles; (2) it is possible to easily perform mass updates by, for example, updating the software version on a whole fleet of vehicles at the same time; (3) it is possible to push out new software to vehicles almost instantly rather than waiting for vehicle owners to bring their vehicles to a workshop to perform the software update; thus reducing the time vehicles with vulnerable software are out on the streets. The requirement for security for this case is clear as attackers could otherwise target weaknesses in the software over-the-air procedure by modifying original software or creating their own software. Some attackers may be motivated to increase or add more features, for example, increase horse power. Malicious attackers may create vehicle virus or worms that ultimately could result in, for example, car accidents. Such malicious software could trigger unwanted behavior in a vehicle such as disabling the brakes when the vehicle reaches a certain speed (Nilsson and Larson 2008).

[1]Tesla Motors is already offering software updates over-the-air for their in-vehicle control modules and have officially handled "recalls" with software updates over-the-air rather than traditional recalls.

Remote diagnostics is another promising case where auto manufacturers would be able to collect information on vehicles remotely and be able to process and analyze such information on a timely basis. The advantages are as follows: (1) while driving a problematic vehicle to the workshop, the workshop technician can perform remote diagnostics to analyze the vehicle in advance and prepare any necessary spare parts; (2) the vehicle owner's waiting time at the workshop is reduced as the analysis has been performed in advance; thus the time to wait is only for the technician to perform the actual work that requires physical access, e.g., to replace a component; (3) the auto manufacturer can more easily and timely collect comprehensive data of vehicle trouble to analyze and identify failure trends on a larger scale in order to reduce future potential failures as well as to better prepare handling of upcoming failures. The need for security for this case is also clear as only authorized users should be able to access and execute certain diagnostics functions within a vehicle. Depending on the type of diagnostics functions, it needs to be carefully considered which security properties are required. Otherwise, attackers could target the remote diagnostics procedure to gain access to sensitive information or worse, cause accidents by executing potentially safety-related function tests (Oka et al. 2014).

V2V communication is communication between vehicles (vehicle-to-vehicle), and V2I communication is communication between a vehicle and its surrounding infrastructure. Such communication is considered useful in several instances, e.g., for efficiently distributing safety warnings, traffic and accident information, as well as to provide support for future use cases such as autonomous driving. For V2V and V2I communication, vehicles can be considered to have gained a new sense in terms of hearing. Vehicles would be able to hear what other vehicles or the infrastructure is telling them. The result is that, something that is not in the line-of-sight of a driver or a vehicle could be communicated. For example, a vehicle suddenly applying the brakes that is two cars ahead and not visible to a certain driver could automatically send a V2V message indicating that the brakes are applied. The driver behind who cannot see as yet the actual vehicle applying the brakes would be able to react appropriately to this message by preparing to brake. One can also consider using smart intersections where the infrastructure could detect pedestrians crossing the street and send V2I messages informing vehicles making a turn at the intersection about any crossing pedestrians. V2V and V2I communication (or collectively known as *V2X communication*) can become increasingly more important as it can be combined with other technologies to provide support for autonomous driving. For example, a vehicle could automatically apply the brakes in above use cases based on the received V2X message (warning about vehicle braking or pedestrian crossing the street). For V2X communication, there is an obvious need for security. If attackers can send false messages, there is a risk that users will lose faith in the system and ignore warnings, which could also lead to accidents. Furthermore, if vehicles react automatically to the contents of messages, for example, in the scope of autonomous driving, an attacker sending false messages could cause vehicles to behave in an undesired way. Therefore, any external messages processed by a vehicle that may affect the

safety of the vehicle are required to be properly secured. For example, features such as automatic braking and automatic parking affect the braking and steering of a vehicle. If an attacker can spoof messages to trigger such features at the wrong time, the attacker could cause accidents with serious consequences to safety. Another concern regarding V2X communication, considering the point of view of drivers, is the potential invasion of privacy. For example, if messages sent from a specific vehicle contain personal information or can be easily tracked, it could lead to serious privacy issues for the driver.

In all of these cases presented above, attackers can target the critical infrastructure that comprises vehicles and their surrounding infrastructure. As shown by the examples above, there is a strong need for security to protect not only the safety of an individual driver in a single vehicle but the safety for everyone involved in the entire infrastructure and all connected vehicles.

14.3 Security Advancements

While considering employing the novel cases presented in previous section, the automotive industry is putting in more effort to better understand security threats and security solutions. For example, several auto manufacturers such as General Motors, BMW and Volkswagen have established dedicated security teams whose sole purpose is to ensure security for automotive solutions. Moreover, several research projects have introduced security solutions in the automotive industry such as automotive-grade hardware security modules. Automotive and industrial organizations such as Society of Automotive Engineers (SAE) and Institute of Electrical and Electronics Engineers (IEEE) are developing security standards specifically targeting the automotive industry. Examples include SAE J3061 and IEEE 1609.2. The SAE J3061 standard presents a "Cybersecurity Guidebook for Cyber-Physical Automotive Systems" which aims to provide high-level guidance and principles as well as information on common security tools and methodologies to address cybersecurity threats for the automotive environment (SAE J3061 2015). The IEEE 1609.2 standard defines security services for messages in dedicated short-range wireless communication in vehicular environments, typically considered for V2X communications (IEEE 1609.2 2013).

14.3.1 Automotive-Grade Hardware Security Modules

Security solutions for software updates over-the-air and remote diagnostics need to provide proper authentication measures. In order to provide such security solutions, a trust anchor where additional security solutions can be built upon is necessary. This trust anchor would be a hardware security module that provides the necessary

functions to allow more advanced security solutions to be applied on top of it. During 2008–2011, as part of a European Framework research project, the EVITA (E-safety vehicle intrusion protected applications) project was conducted. The focus of the EVITA project was investigating hardware security solutions appropriate for an automotive setting. The project took into consideration several automotive industry aspects such as stringent cost limitations as well as considering high temperatures and vibrations of hardware in the vehicle to provide an automotive-grade hardware security architecture. The deliverables of the project describe three levels of EVITA hardware solutions (EVITA 2011). Please note that the outcome of the project was a set of documents providing design level specifications for the three levels of hardware solutions: EVITA *Full*, EVITA *Medium* and EVITA *Light*.

The reason for the three different levels is so that the automotive industry can employ the necessary level suitable for the use case in question. In short, the Full version provides the most support for security functionality and supports, for example, both asymmetric and symmetric crypto accelerators in hardware. It is suitable to be used for security solutions where asymmetric crypto accelerator is required, for example, V2X communications. The Medium version is similar to Full except that there is no asymmetric crypto accelerator in hardware. Medium is suitable for providing most security solutions needed in a car. The Light version is simple and basically only has a symmetric crypto accelerator in hardware. It is suitable for providing security solutions that are based on the built-in crypto engine, such as encrypting or decrypting certain pieces of data. It is envisioned that in a car, there will be multiple EVITA level ECUs: e.g., V2X station using Full, Engine ECU, Gateway ECU, Immobilizer using Medium, and Brake ECU, Door ECU using Light.

Using secure hardware as a base, it is possible to build security solutions on top and establish secure protocols based on, for example, standard cryptography to enable and support use cases such as software updates over-the-air and remote diagnostics procedures.

14.3.2 Secure V2X Communications

From 2011 to 2015, there was another European Framework research project called PRESERVE (preparing secure V2X communication systems) that garnered international attention. The purpose of the PRESERVE project is to investigate and identify security solutions for wireless vehicular communication, namely V2X. The PRESERVE project not only considers the fundamental research of security solutions suitable for V2X but also considers the actual implementation, testing and deployment of such solutions. As a result, a complete and close-to-market solution will be provided at the conclusion of the project. The PRESERVE solution includes a security software stack for message handling, security hardware in terms of an application specific integrated circuit (ASIC) implementation including crypto acceleration and secure key storage, and a security backend powered by a complete

public key infrastructure (PKI) solution. In addition, there are ongoing field operational testing at several locations in both Europe and the U.S. to investigate scalability and feasibility issues. Moreover, the V2X security subsystem will be integrated with various solutions from other projects to further investigate integration and performance on larger fleets of vehicles.

To enforce security in V2X systems, there are two main requirements: (1) ensure that a message originates from a trustworthy and legitimate device; and (2) ensure that a message has not been modified between sender and receiver. By applying a PKI solution, where a trusted certificate authority (CA) serves as a trust anchor, V2X stations can securely receive certificates and private keys from the CA. When two V2X stations exchange messages, for example, a car sending a message to another car, the message is digitally signed by the sender to guarantee integrity and authenticity of the message and the corresponding certificate is provided together with the message in the transmission. The receiving V2X station can first verify the authenticity of the received certificate to ensure it has been issued by the trusted CA, and then use the public key included in the certificate to verify the authenticity of the incoming message. This approach fulfills the two main requirements presented above.

However, if a V2X station is using the same private key to digitally sign messages for a long period of time, it could become subject to tracking which could lead to attacks on privacy. Therefore, the suggested approach is to use two types of certificates: long-term certificates and pseudonym certificates (PRESERVE 2015). The long-term certificates serve as the long-term identity of the V2X station. The pseudonym certificates are used in the typical everyday communication between V2X stations. A V2X station has multiple pseudonym certificates and can switch between them after a certain amount of time. Therefore, privacy can be preserved by making it more difficult to track the communication associated to a particular V2X station.

In order to achieve secure V2X communications using this approach, there are several requirements: a large number of pseudonym certificates are required, secure storage of secret keys is required and high performance processing of messages is required. The current approach considers using 20–40 pseudonym certificates per week. As a result, 1000–2000 pseudonym certificates are necessary per year. These certificates are required to be stored on the V2X station, and in order to protect the corresponding private keys, a special key store based on hardware security is necessary. Moreover, there are extremely high performance requirements for V2X security, especially, if the messages are safety related. The current requirement is to be able to process about 200–400 messages per second (e.g., 20–40 vehicles within sending range transmitting 10 messages per second) but actual requirement may vary from OEM to OEM. The bottleneck for a V2X station is the computational-heavy signature verification which would be too slow to perform solely based on software solutions. Consequently, special hardware security in terms of cryptographic accelerators is required. Considering both the hardware security requirements for secure key store and cryptographic accelerators, the corresponding required EVITA level for a V2X station is EVITA Full.

14.3.3 Secure In-Vehicle Network Communications

Even if external communication with the vehicle can be secured, considering the defense-in-depth principle appropriate security measures for prevention, detection, deflection and countermeasures are required (Larson and Nilsson 2008), and thus a multi-layered security approach by implementing security for the in-vehicle network communication is required. As has been demonstrated by security researchers already, by accessing the in-vehicle network and sending messages on the CAN network, it is possible to take control of various safety-critical vehicle functions such as enabling or disabling brakes or causing the steering wheel to turn (Koscher et al. 2010; Miller and Valasek 2013). AUTomotive Open System ARchitecture (AUTOSAR), a partnership of OEMs, tier 1 suppliers and other companies from industries such as semiconductor and software, is working on standardization of basic software functions of automotive ECUs and an open architecture platform upon which future vehicle applications can be implemented. Among its vast body of work, AUTOSAR has also recognized the challenge of secure in-vehicle network communication and as a result developed a specification for secure onboard communication released in AUTOSAR 4.2.1 (AUTOSAR 2014).

The AUTOSAR Secure Onboard Communication (SecOC) specification takes into consideration the resource-constrained devices existing in typical in-vehicle networks and thus provides resource-efficient and appropriate authentication mechanisms for critical data transmitted on the in-vehicle network. The specification considers mainly symmetric authentication approaches using message authentication codes (MACs). The SecOC specification provides authentication and integrity protection, i.e., ensuring that received data comes from the correct ECU and has not been modified. Moreover, freshness protection in the exchanged messages is also supported by the SecOC specification. The security solution is specified as follows. Both sending and receiving ECU need to implement a SecOC module. To provide freshness protection, the respective SecOC modules maintain freshness values (e.g., freshness counters or timestamps). Both sending ECU and receiving ECU need to store the same shared secret key. The sending ECU first creates authentication information in form of an Authenticator (e.g., MAC). The Authenticator is a piece of unique authentication data calculated using the actual message, a secret key and the freshness value as inputs to a MAC generation algorithm. The payload for a message then consists of the actual message concatenated with the freshness value and the Authenticator. The length of the full message may vary depending on the desired security level and performance requirements. For instance, the SecOC specification allows truncating the Authenticator to reduce the length of the message. This allows flexibility in the system to support various messages types with different Authenticator lengths.

The sending ECU transmits the payload containing the actual message, freshness value and Authenticator to the receiving ECU. The receiving ECU first verifies that the received freshness value is higher than the locally stored freshness value, i.e.,

the received message is new and not a replay of an old message. The receiving ECU then performs MAC verification by using the received actual message, received freshness value and the same secret key as inputs to generate the MAC and verifies if the received MAC matches the calculated MAC. If the comparison is successful, the receiving ECU can be assured that the message originates from the correct ECU (sharing the same secret key), that the message has not been modified and that the message is current (i.e., not replayed).

If truncated Authenticator values are used, only parts of the MAC are transmitted and compared, resulting in a lower security level. Regarding the truncated Authenticator size, National Institute of Standards and Technology (NIST) considers MAC sizes of 64 bits and above to provide sufficient protection against guessing attacks. However, security experts should carefully consider the appropriate length of truncated MACs when deciding on the MAC sizes to ensure a desired level of security for the various use cases is achieved. Furthermore, suggested algorithms for calculation of the Authenticator include advanced encryption standard cipher-based message authentication code (AES-CMAC) especially for use cases involving resource-constrained devices.

14.3.4 Embedded Security Evaluation

Another topic that has garnered attention lately is embedded security evaluation. For example, by applying in-depth security evaluations of automotive components such as ECUs early in the development cycle, it would be possible to identify and remedy potential security weaknesses before actual attackers in the field could exploit such weaknesses and cause potentially high financial and safety damage.

Basically, there are two categories of security evaluations: theoretical and practical. Theoretical security evaluations can and should be performed during all steps of the automotive development cycle, ideally starting as early as possible in the development cycle, whereas practical security testing, can only be performed when an implementation of the target system is available, such as a prototype device. Examples of theoretical security analyses include design analysis and threat and risk analysis. A design analysis is often a more high-level analysis based on some high-level descriptions of an automotive system. The goal of the design analysis is to identify systematic flaws in the system at an early stage in the development cycle by searching for potential attack vectors such as weak cryptographic algorithms or weaknesses in interactions between standard protocols. When more documentation about the automotive system is available, a more in-depth threat and risk analysis can be conducted. Here, the system is first analyzed more thoroughly and possible attacks and their associated risks are identified. Any security weaknesses that are associated with high risks need to be considered as the weaknesses with the highest priority to be fixed first. However, theoretical security analyses cannot find any

implementation flaws or deviations from the implementation from the specification. To reduce the risk of implementation issues, secure software development processes should be followed (CERT 2014; SAFECode 2011).

Even if best practices for secure development processes are followed, there might still be vulnerabilities in the implementation. Practical security testing can be applied to find such vulnerabilities. A thorough practical security test helps to establish trust in the soundness of an implementation as it can find unspecified functions and discrepancies to the specification. Moreover, practical security testing provides an understanding of how difficult it would be to actually conduct a certain attack against the target system, thus giving an indication of how difficult it would be for a real attacker to perform the same attack. A typical security test comprises four steps. The first step is *functional security testing* which focuses on testing the correct behavior and robustness of all security-relevant functions in the target system. This step can reveal implementation errors, discrepancies to the specifications as well as unspecified functionalities that may lead to security weaknesses. The second step is called *vulnerability scanning* where the target system is tested for known common security vulnerabilities. Examples include known security exploits and inappropriate configurations that contain known weaknesses. The next step goes deeper and focuses on finding unknown security vulnerabilities. This step is called *fuzzing*. It is performed by sending malformed or out-of-specification input to the target system and monitoring the resulting behavior to identify any unknown and potentially security-critical system behavior. Finally, the last step focuses on testing the system as a whole by performing *penetration testing* targeting both the software and the hardware of the target system. In this step, a human tester mimics a resourceful attacker by trying to exploit all previously found security vulnerabilities. The human tester uses years of "hacking experience" to reverse-engineer, extract useful or secret data, and combine several software and hardware-based approaches to create more sophisticated attacks. For example, exploit a hardware debug interface weakness to dump certain parts of memory and use software-based attacks to extract secret keys and other useful data.

It is important to note, however, that it is extremely difficult to give any assertion on completeness for practical security testing, especially for fuzzing and penetration testing. It is necessary instead to decide on the amount of effort that will be dedicated for this type of testing in terms of time, scope and resources. As a result though, it may be possible that such testing will miss to identify major systematic flaws. Therefore, practical security testing cannot replace theoretical security analyses but instead should be complemented by theoretical analyses to ensure a more complete coverage of security testing. Also, as mentioned previously, the entire software development process should be improved to include security at all stages of the development cycle by employing a secure development practice to minimize the total attack surface early on in the process (Bayer et al. 2015).

14.4 Summary and Conclusions

With advancements in technology and introduction of new use cases in the automotive domain, there are security solutions under development or already deployed in the field. First, automotive hardware security based on EVITA, is the foundation of all automotive security solutions. It serves as a trust anchor where additional security solutions can be built upon and provides necessary hardware crypto acceleration to support real-time performance requirements in automotive network communication and processing. V2X communication is protected based on established industry standards both in terms of assuring authenticity of exchanged messages as well as preserving privacy of drivers. For in-vehicle network communications, AUTOSAR has released the 4.2.1 standard which includes a SecOC module responsible for secure in-vehicle network communications. Last, evaluations of embedded security are becoming increasingly important, and especially it is necessary to consider not only theoretical evaluations such as threat and risk analysis, but also practical security testing such as fuzzing and penetration testing. Applying the necessary hardware and software security solutions would enable the automotive industry to prevent cyber security attacks on vehicles as well as allow new business opportunities. It would be possible to prevent illegal chip-tuning, manipulation of the odometer and spoofing of messages in both V2X and in-vehicle network communications. Moreover, it would be possible to introduce new business opportunities, such as software updates over-the-air and remote diagnostics. Although there are some security solutions already available and more solutions in development, there are some challenges in terms of time and cost before the automotive industry can start to fully implement these solutions. Furthermore, one can imagine that there will be misconfigurations, user errors and software vulnerabilities in the implemented solutions, as well as a new breed of more innovative attacks as attackers learn more about the systems. As a result to protect against such future attacks, automotive security solutions will need to constantly evolve. To conclude, automotive trends such as the *connected car* will be realized in the future but will require proper security solutions to be in place first. This chapter has given a few examples of automotive security solutions that need to be considered to secure a critical infrastructure such as transportation systems.

References

ADAC. (2014). *ADAC recommendations for the 2014 European elections*. Online: http://www.adac.de/_mmm/pdf/fi_europawahl2014_engl_broschuere_0414_207126.pdf

AUTOSAR. (2014). *Specification of module secure onboard communication.* Online: http://www.autosar.org/fileadmin/files/releases/4-2/software-architecture/communication-stack/standard/AUTOSAR_SWS_SecureOnboardCommunication.pdf

AUTOWEEK. (2013). *Cyber threats targeting your car*. Online: http://autoweek.com/article/car-news/cyber-threats-targeting-your-car

Bayer, S., Enderle, T., Oka, D. K., & Wolf, M. (2015). Security crash test—Practical security evaluations of automotive onboard it components. In *Automotive safety & security*.

CERT. (2014). *Secure coding standards*. Online: http://www.cert.org/secure-coding/research/secure-coding-standards.cfm

Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F., & Kohno, T. (2011). Comprehensive experimental analyses of automotive attack surfaces. In *Proceedings of the 20th USENIX Conference on Security*.

EVITA. (2011). *EVITA deliverables*. Online: http://www.evita-project.org/deliverables.html

Greenberg, A. (2015). *Hackers remotely kill a jeep on the highway—With me in it*. Online: http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Howard, B. (2012). *Hack the diagnostics connector, steal yourself a BMW in 3 minutes*. Online: http://www.extremetech.com/extreme/132526-hack-the-diagnostics-connector-steal-yourself-a-bmw-in-3-minutes

IEEE 1609.2. (2013). *1609.2-2013—IEEE Standard for wireless access in vehicular environments—Security services for applications and management messages*.

IQPC. (2012). *The changing face of car theft: A motivation to improve car security*. Online: http://www.automotive-iq.com/PDFS/Electronic%20theft%20article%20by%20SBD.pdf

Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., & Savage, S. (2010). Experimental security analysis of a modern automobile. In *Proceeding of IEEE Symposium on Security and Privacy*.

Larson, U. E., & Nilsson, D. K. (2008). Securing vehicles against cyber attacks. In *Proceedings of the Fourth ACM Cyber Security and Information Intelligence Research Workshop*.

Markey, E. (2013). *As wireless technology becomes standard, Markey queries car companies about security, privacy*. Online: http://www.markey.senate.gov/news/press-releases/as-wireless-technology-becomes-standard-markey-queries-car-companies-about-security-privacy

Markey, E. (2015a). *Markey report reveals automobile security and privacy vulnerabilities*. Online: http://www.markey.senate.gov/news/press-releases/markey-report-reveals-automobile-security-and-privacy-vulnerabilities

Markey, E. (2015b). *Sens. Markey, Blumenthal introduce legislation to protect drivers from auto security, privacy risks with standards & "cyber dashboard" rating system*. Online: http://www.markey.senate.gov/news/press-releases/sens-markey-blumenthal-introduce-legislation-to-protect-drivers-from-auto-security-privacy-risks-with-standards-and-cyber-dashboard-rating-system

Markey, E. (2015c). *SPY Car Act*. Online: http://www.markey.senate.gov/imo/media/doc/SPY%20Car%20legislation.pdf

Miller, C., &Valasek, C. (2013). Adventures in automotive networks and control units. *DEFCON*, *21*.

Miller, C., & Valasek, C. (2014). A survey of remote automotive attack surfaces. *DEFCON*, *22*.

NHTSA. (2015). *NHTSA and vehicle cybersecurity*. Online: http://www.nhtsa.gov/About+NHTSA/Speeches,+Press+Events+&+Testimonies/NHTSA+and+Vehicle+Cybersecurity

Nilsson, D. K., & Larson, U. E. (2008). Simulated attacks on CAN buses: Vehicle virus. In *Proceedings of the Fifth IASTED International Conference on Communication Systems and Networks*.

Oka, D. K., Furue, T., Bayer, S., & Vuillaume, C. (2014). Analysis of performing secure remote vehicle diagnostics. In *Proceedings of Computer Security Symposium 2014*.

PRESERVE. (2015). *PRESERVE—Preparing secure V2X communication systems*. Online: https://www.preserve-project.eu/deliverables

SAE J3061. (2015). Cybersecurity guidebook for cyber-physical automotive systems.

SAFECode. (2011). *Fundamental practices for secure software development*. Online: http://www.safecode.org/publication/SAFECode_Dev_Practices0211.pdf