Protecting Our Future

Volume 2

Protecting Our Future, Series in Cybersecurity
Editor, Jane LeClair

Protecting Our Future: Educating a Cybersecurity Workforce, Vol. 1
Examines 7 of the 16 Homeland Security Critical Infrastructure Sectors, in addition to other workforce needs.
Edited by Jane LeClair

Cybersecurity in Our Digital Lives
Looks at evolving operational needs in areas that affect our daily digital lives.
Edited by Jane LeClair and Gregory Keeley

Protecting Our Future: Educating a Cybersecurity Workforce, Vol. 2
Examines 9 of the 16 Homeland Security Critical Infrastructure Sectors.
Edited by Jane LeClair

Protecting Our Future

Educating a Cybersecurity Workforce

Volume 2

edited by

JANE LECLAIR

HUDSON WHITMAN

EXCELSIOR COLLEGE PRESS

Published in the United States by
Hudson Whitman/ Excelsior College Press
7 Columbia Circle, Albany, NY 12203
www.hudsonwhitman.com

Printed in the United States of America
Book design by Sue Morreale
Cover design by Philip E. Pascuzzo

Library of Congress
Cataloging-in-publication data
LCCN 2013950476
Print ISBN: 978-0-9898451-6-8 (paperback)

Contents

Acknowledgments

Every publication from the National Cybersecurity Institute is, of course, the result of a team effort. No one person can possibly complete a work such as this without a great deal of assistance and support. The team at NCI worked together planning, selecting the topics, locating the writers, encouraging them to meet their deadlines, editing their submissions, and publishing the final product. Special thanks go to Denise Pheils and James Antonakos for their proofreading and moral support along the way. Thanks to the publishing and production team at Hudson Whitman, including Susan Petrie, Sue Morreale, Wendy Catalano, and Phil Pascuzzo. The greatest of appreciation goes to the many writers who contributed so much of their time and talent in writing their individual chapters. As always, the president of Excelsior College, Dr. John Ebersole, must be thanked for his ongoing support and enthusiasm for the National Cybersecurity Institute.

Foreword

The security and prosperity of our great nation have been and must continue to be our highest priority. Rapid and ongoing advances in communication technology have brought convenience to our everyday lives, but at the same time have made us vulnerable to foreign and domestic actors with malicious intent.

During my tenure within the Department of Defense as Director of the National Security Agency/Central Security Service Threat Operations Center (NTOC), I witnessed the increasing volume, sophistication, and pervasiveness of the cyber threat. Now, in my role as a senior advisor at CyberPoint International, I witness exploitation, disruption, destruction, and subjugation. Over the years, the target set has dramatically expanded from government to commercial entities to critical infrastructure, and to individual citizens. And, there is significant growth in the number and type of perpetrators, from nation states to hacktivists to terrorists, even individuals for hire.

The scope of the cyber threat is broad—spanning sensitive /classified government data and operations to our most personal financial and medical information. The threat also includes our critical infrastructures, those things that we take for granted like power, water, emergency services, and food supply. A cyber-attack on any of these would have a catastrophic effect on our very way of life.

We must proactively consider these risks.

Sherri W. Ramsay

Introduction

Jane LeClair

As we all are aware, cybersecurity continues to be one of the most talked about issues of our time. Hardly a week goes by that one organization or another does not have its digital network breached. Big box retailers such as Target, Home Depot, Michaels, and Neiman Marcus have been attacked. Financial institutions like JP Morgan, Bank of America, SunTrust, Wells Fargo, and U.S. Bank have been hacked. Newspapers like the *New York Times* and the *Wall Street Journal* saw hackers disrupt their operations, and newspapers in Paris were hacked following terrorist attacks. On the federal government level, the Office of Personnel Management, the United States Postal Service, the State Department, the National Oceanic and Atmospheric Administration and the Energy Department have had their digital systems attacked. Even the cyber system of the White House was breached. With so many breaches in the news it is small wonder why the conversation in the cyber community is so active with discussion on threats and efforts to mitigate them.

Increasingly the attention of the cyber community has been focusing on the threats to the critical infrastructure of the country. While threats to retailers, movie studios, and newspapers should not be discounted or downplayed, the important infrastructures that bind the nation together are having the spotlight turned on them for

protection. Presidential Policy Directive (PPD-21) released in 2013 identified sixteen critical infrastructures that needed immediate and ongoing cyber protection for the nation to continue to function. Those sixteen identified infrastructures are: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials, and Waste; Transportation Systems; and Water and Wastewater Systems. Each is vital for the economic prosperity and survival of the nation and each is increasingly vulnerable to cyber-attacks.

In the first volume of *Protecting Our Future* a distinguished group of writers provided their insights into several critical infrastructures, including: finance, health care, government agencies, and communications. In volume two of *Protecting Our Future*, we will be taking a close look at additional sectors of our critical infrastructure. The National Cybersecurity Institute (NCI) in Washington, D.C., in conjunction with Excelsior College, has once again collected an outstanding group of authors who are recognized for their expertise in their sectors. The sectors that are addressed in this publication are information technology, the chemical industry, commercial facilities, critical manufacturing, water and dams, emergency services, food and agriculture, transportation. The last chapter examines future directions for educating a cybersecurity workforce.

In the first chapter, Dan Shoemaker and Anne Kohnke address the very unique issues that are involved with information security and cybersecurity. Much of our society is interconnected with technology and information. Keeping all the data that is stored in countless servers safe, yet readily available, is a relentless ongoing task. The authors will bring the reader up to date on the latest developments in securing your data, discuss the fundamentals of cybersecurity, common cyber threats, and the skills required to help mitigate those threats. They will also address the numerous rules and regulations that govern the arena of cybersecurity.

We rely heavily on chemicals in most of our manufacturing processes and by their very nature and importance they require special care. Currently there are approximately ten thousand organizations

involved in the chemical industry employing nearly a million people and producing more than seventy thousand products that are utilized on a daily basis. In chapter two, George (Buzz) Murphy examines this critical portion of our infrastructure, its importance to our economy, the threats it faces, and what must be done to protect its viability. The cyber threat to the chemical industry is a serious one, and the incorporation of increasing amounts of technology into the operating systems of the industry has greatly enhanced opportunities for hackers. The author makes special note of how the Internet of Things (IOT) and Machine to Machine (M2M) technologies may increase vulnerabilities.

Our commercial facilities are constantly under assault by bad actors, and in chapter three Denise Pheils and Randy Sylvertooth offer expertise on how seriously they are taking the issue and what steps are being taken to secure commercial data. The authors note that commercial infrastructure encompasses numerous sub-sectors we are all familiar with: sports, entertainment and media, outdoor events, gaming, public assembly, lodging, real estate, and retail spaces. Each has unique security requirements.

In chapter four, Kevin McLaughlin offers a perspective on cybersecurity in the manufacturing sector as it pertains to commodities. Increasingly, the Critical Manufacturing Sector has been turning to automation to more efficiently produce our goods and maintain market share in an increasingly competitive global economy. This reliance on automation, driven by technology and advanced computer systems, increases the likelihood of a cyber-attack by those seeking to disrupt that essential infrastructure. He warns the C-Suite not to be complacent about their organization's cybersecurity because compliance with regulations does not necessarily guarantee security.

We can do without many things, but we cannot exist long without water. In chapter five, Philip Burnett offers insight into how our water system operates, how our dams are controlled with technology, and how vital it is to protect them from malicious intent. In his chapter, "The Dams Sector and the Water and Wastewater Systems Sector," Burnett details the SCADA-based control systems that are increasingly being utilized in the water and dams critical infrastructure.

We all know how important it is to have someone respond to our 9-1-1 calls and provide the emergency services we have come to take for granted. In chapter six, William Martin presents an overview of emergency services, how they operate, and steps that are being taken to secure them. Emergency services go beyond the immediate response to a life-threatening emergency, they also include the restoration of vital services should they be disrupted.

Our food supply is also critical. The supply chain for produce, dairy products, and livestock is complex and relies heavily on technology. For example, the selection of seed, its delivery, appropriate care during growth, harvest, and transport to the marketplace all require reliance on technology. Christina Cooper provides a unique perspective on this area in chapter seven and offers her insights on cybersecurity laws, policies, and guidelines.

Kin Wong takes us through the Transportation Sector in chapter eight, and looks at the interconnected role of how commodities move, how fuel is delivered, how food is shipped, traffic controlled, and what keeps trains running on schedule. He provides us with several important recommendations: establishing common cyber standards in aviation, understanding threats and risks, and developing a culture of cyber awareness—one that is situational and responsive in the event of a breach.

Finally in chapter nine, Kyle Foley continues our discussion of future directions for educating a cybersecurity workforce. He concludes by offering recommendations for best practices across the sectors.

Volume one of *Protecting Our Future* looked at several sectors that had received scant attention, including small business, education, training, government, and healthcare. This volume continues that effort and addresses numerous sectors that have, until now, not been adequately discussed. Our critical infrastructures have been identified as those which are essential to our safety, well being, and the continued success of our national economy. Each sector is critical. By increasing the awareness of the value of our critical infrastructures, we can better prepare their defenses.

The National Cybersecurity Institute, in conjunction with Excelsior College, is once again pleased to bring together a collection

of cyber and subject matter experts who have pooled their talents to produce this current work. As media headlines continually showcase the many cybersecurity issues that organizations are facing, this work is both timely in raising awareness of these issues and at the same time offers suggestions as to how those issues might be mitigated.

A recent proclamation from the White House stated:

> Critical infrastructure protection is an essential element of a resilient and secure nation. Critical infrastructure are the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety.

It is firmly hoped that this publication will contribute to the security of those vital assets.

References

Aspan, M. (2012, September 27). Bank data breaches are stuff of nightmares: Citi exec. *American Banker*. Retrieved from http://www.americanbanker.com/people/bank-data-breaches-are-stuff-of-nightmares-citigroup-executive-1053085-1.html

Barbash, F. and Nakashima, E. (2014, July 10). Chinese hackers may have breached federal government's personnel office, U.S. officials say. *The Washington Post*. Retrieved from http://www.washingtonpost.com/news/morning-mix/wp/2014/07/09/report-chinese-hacked-into-the-federal-governments-personnel-office/

Burnett, R. (2006, April 21). Banks scramble after cyber-breach. *Orlando Sentinel*. Retrieved from http://articles.orlandosentinel.com/2006-04-21/news/CARDBREACH21_1_debit-suntrust-account-numbers

Eagan, M., & Booton, J. (2013, August 14). Source: New York Times Website hit by cyber attack. Fox Business. Retrieved from http://www.foxbusiness.com/technology/2013/08/14/new-york-times-site-experiences-major-outage/

Nakashima, E. (2014, November 10). China suspected of breaching U.S. postal service computer networks. *The Washington Post*. Retrieved from http://www.washingtonpost.com/blogs/federal-eye/wp/2014/11/10/china-suspected-of-breaching-u-s-postal-service-computer-networks/

NBC News. (2014, November 16). State Department joins growing list of hacked federal agencies. Retrieved from http://www.nbcnews.com/news/us-news/state-department-joins-growing-list-hacked-federal-agencies-n249711

The White House (2009, December 2). Presidential proclamation—Critical Infrastructure Protection Month. Retrieved from http://www.whitehouse.gov/the-press-office/presidential-proclamation-critical-infrastructure-protection-month

Voight, K. (2013, February 1). Chinese cyber attacks on West are widespread, experts say. CNN. Retrieved from http://www.cnn.com/2013/02/01/tech/china-cyber-attacks/index.html

Wn.com (2015, January 16). Charlie Hebdo: French newspapers hit by cyberattacks after Paris shootings, with sites including Le Parisien. Retrieved from http://article.wn.com/view/2015/01/16/Charlie_Hebdo_French_newspapers_hit_by_cyberattacks_after_Pa/

Chapter 1

Cybersecurity and Information Technology

Dan Shoemaker and Anne Kohnke

Introduction: What is Cybersecurity?

The Internet age has produced jargon including the term "cybersecurity." A few attempts to define cybersecurity by researchers and IT security professionals include:

- Cybersecurity involves human intelligence—exploits and vulnerabilities are created to defy and change the rules of systems they target (Toecker, 2014).
- Cybersecurity is nongeographical, it is epiphenomenal and a consequence of the computer and Internet revolution and a problem unlike any other security problem the nation has faced before (Harknett and Stever, 2011).
- Cybersecurity tends to be used as a synonym for information systems security encompassing identity and access management, breach incident response and the protection of information technology infrastructure such as networks, routers, e-mail, and Web servers (Bissell, 2013).

Although there are many definitions, the one thing hackers target is information in the form of electronic data and the aim for organizations is protection. The measures themselves are undefined but their purpose is clear: to prevent loss or harm to information that is stored on an electronic device. Therefore, it might be safe to conclude that the field of cybersecurity embraces any appropriate measure to ensure that electronic data is kept safe from unauthorized access or harm. In simpler terms, cybersecurity safeguards the information that is processed, in transit, and at rest or stored on computers. The processes, technologies, and practices in the field of cybersecurity are designed to safeguard assets which includes the efforts of professionals to create unbreakable defenses against penetration of the electronic perimeter. These types of attacks are often termed "hacking." Additionally, should the electronic boundary be breached, a good cyberdefense should detect and defend against intrusions, by preventing loss or harm to the data (Shoemaker & Kennedy, 2009). When implemented properly, a good cybersecurity defense should include the following:

- Accurately identify and authenticate all entities seeking access to a system.
- Authorize access to only those objects that the entity's level of trust permits.
- Monitor and control activities during the time that the entity is granted access.
- Ensure against unauthorized access, or manipulation of data.
- Ensure against unauthorized manipulation of system objects.

Fundamental Issues Unique to Information Technology

Security of information is a crucial concern in a world where "terrorism" has become a household word. Cybersecurity is especially impor-

tant because every part of our economy depends on some kind of information asset; therefore, advancing our capability in safeguarding those assets is a vital national interest. Cybersecurity is an increasingly important issue in our society because threats continue to grow while at the same time America's electronic infrastructure is riddled with a growing number of vulnerabilities. That exponential growth in exploitations greatly increases the risk to our way of life (Moran, 2013).

According to the Privacy Rights Clearinghouse (PRC) (2014), over one billion records have been lost during the past ten years. The running average of 100 million records lost per year has been subject to some variation over time and the source of breach has changed. What is worse, these figures only include breaches that were reported. Since most companies do not like to publicize their security failures, that number could be significantly higher. Each of these incidents represented a discrete event that entailed one of four attack types: unauthorized access, malicious code, denial-of-service, and inappropriate usage (PRC, 2014). The number of reported incidents has risen annually from 108 in 2005, to 607 in 2013 (PRC, 2014). This information suggests that the number of successful incidents has risen almost six-fold over the past decade. There are many factors that underlie these statistics, but the direction is clear. The need for an effective and continuously evolving cyberdefense is an absolute imperative. Unfortunately, the evidence so far indicates that global interconnectedness and the propagation of hacker tools means that today's computer systems are actually less secure than a decade ago (Pfleeger & Rue, 2008).

The U.S. General Accounting Office (GAO) has conducted a thorough study aimed to identify challenges in addressing a strategic approach to cybersecurity, and found significant weaknesses in the national information infrastructure. Moreover it hypothesized that, as the body of audit evidence grows, it is likely that . . . "additional significant deficiencies will be identified" (GAO, 2014).

The six major findings of the GAO study were:

1. Risk-based security plans not developed for major systems

2. Security policies not documented
3. Programs for evaluating the effectiveness of controls not implemented
4. Controls for application development and change control not implemented
5. Inadequate control over the implementation and use of software products
6. No expertise to select, implement, and maintain security controls (GAO, 2014)

The overall problem highlighted by the GAO is that protection of our electronic infrastructure is not a simple issue of computer security. The breaches that fall under the domain of traditional computer security, including network and operating system assurance, comprise only 29% of the total source of breach. The other 71% can be attributed to attacks that exploit human behavior, commonly called "social engineering," and outright physical attacks, such as loss or theft of laptops, personal devices, or media (PRC, 2014). What these statistics imply is that, until all avenues of attack have been safeguarded it cannot be stated that the electronic infrastructure is protected. Adoption of better and more effective ways to protect our information are necessary.

This chapter will present the fundamental concepts of how to accomplish this goal. This approach is termed "holistic" in its focus lifecycle. Holistic cybersecurity demands complete protection from all forms of attack, both electronic and behavioral. The concepts in this chapter constitute a survey rather than a listing of best practices in every area of the field. This chapter begins with a discussion of the threats to information technology.

Cybersecurity Threats that Challenge Information Technology

Threats vary with the definition of responsibility. Obviously, the threats will be different if the only goal of cybersecurity is to protect the computer and the networks attached to it. If the goal is to protect the

overall information infrastructure from all forms of attack, the types and number of threats will vary. The issue of threat is a matter of mission and scope. There are numerous threats to computers and networks. One of the best references for identification of threats is the Common Weakness Enumeration—CWE (Martin, 2014). At present, the CWE lists 999 root causes that can be expanded to 6,000 actual weaknesses (Martin, 2014). Nevertheless, when you factor in every other way that a computer can be threatened, including insider action, social engineering, and physical access attacks such as theft, the number of threats becomes almost uncountable. The focus in threat mitigation is on best practices, which install protection processes that are generally acknowledged within the industry and believed to work. There are a number of commonly accepted standards that define such practices. Perhaps the two standards with the greatest impact are ISO 27000 and FIPS 200.

The ISO 27000 suite of standards provides the world's categorization of the types of threats to information systems (ISO, 2012). The standard was developed by the International Standards Organization (ISO) over an extended period of time culminating in its initial publication in 2005 (ISO, 2012). The current standard, ISO 27000, is the 2014 version. This standard specifies 14 areas of control considered a classification of the general types of threats. There are 135 explicit controls specified within these general areas and the process for defining additional controls is provided. The U.S. has its own model, which was developed in response to the Federal Information Security Management Act (FISMA) (FISMA, 2002). This model is referred to as the FIPS 200 Framework (NIST, 2014a). FIPS 200 describes the steps needed to satisfy the requirements of FISMA and serves the same purpose as ISO 27000 in that it describes areas of threat and common control practices to meet those threats. There are 17 specific categories of threat specified in FIPS 200. The recommended practices for dealing with those threats are contained in NIST 800-53 (NIST, 2014b). The National Institute of Standards and Technology has written an extensive and thorough document outlining over 100 pages of controls (NIST, 2014b).

Shown in Table 1.1 below, there is a 93% overlap between ISO 27001 and FIPS 200, which rather persuasively indicates that the areas outlined must be taken into consideration when considering a cybersecurity solution.

Table 1.1. Comparison of ISO 27001 and FIPS 200 Security Control Categories (Shoemaker & Kohnke)

ISO 27001	FIPS 200
Information Security Policies	Planning (PL)
Organization of Information Security	Audit and Accountability (AU)
Human Resource Security	Personnel Security (PS)
Asset Management	Identification and Authentication (IA)
Access Control	Access Control (AC)
Cryptography	Physical and Environmental Protection (PE)
Physical and environmental security	System and Information Integrity (SI)
Operation Security	System and Communications Protection (SC)
Network security management	Maintenance (MA)
Security in development and support	System and Services Acquisition (SA)
Supplier relationships	Incident Response (IR)
Incident management	Contingency Planning (CP)
Business continuity management	Certification, Accreditation, and Security Assessments (CA)
Compliance	Risk Assessment (RA)
	Awareness and Training (AT)
	Media Protection (MP)
	Configuration Management (CM)

To simplify the terminology, the following are areas requiring countermeasures from common threats:

- Policy
- Governance control
- Personnel security

- Physical and environmental security
- Asset management
- Access control
- Security of operations
- Network security
- Computer security
- Software development and maintenance security
- Acquisition
- Incident management
- Compliance
- Continuity
- Elements of human factors including training and education

This list is considered to be a summary of the potential threat vectors in any cybersecurity situation. Any or all of these areas need effective countermeasures in place in order to protect against the types of threats that might be identified for each category. The controls suggested by each of these standards can serve as a point of reference for developing a tailored cybersecurity response. However none of these will be effective unless the organization undertakes a comprehensive analysis of the threat environment using some form of checklist developed from the selected control set. The ability to perform risk assessments and develop an effective real-world cybersecurity protection scheme depends on the knowledge and abilities of the people doing the work. Therefore there is considerable interest in the development of a skilled and knowledgeable workforce. Because the field is new, the need for trained workers exceeds the supply. As a result, the International Information Systems Security Certification Consortium ((ISC)^2) Global Workforce Survey predicts that the growth of the cybersecurity workforce will be in the neighborhood of 14% for the

foreseeable future (Suby, 2013). Opportunities abound for people looking for careers in cybersecurity.

Cybersecurity Laws Relevant to Information Technology

Legal and regulatory considerations as part of cybersecurity may seem odd, however cyberlaw is important in an era where the failure to exercise adequate due diligence, or comply with the requirements of a law, regulation, or contract can bring significant harm to the organization. Law in cyberspace encompasses any action involving the fulfillment of the terms of a contract, meeting the requirements of law, satisfying an applicable regulation, and meeting a mandated standard. Thus, the term "cyberlaw" describes conformance with applicable laws, regulations, and contracts. Most of the laws that have been passed to-date have to do with protecting privacy or regulating commercial transactions using computers. They all have something of a governmental and bureaucratic focus. These regulations can be classified into four generic categories:

- governmental regulations
- privacy regulations
- laws that regulate computer crime
- laws that regulate classified or sensitive information

Much of the legal action over time concerns defining the rights of individuals. Based on legal precedents that have evolved over the past 40 years, individuals have the right to control some but not all of their information. Many legal precedents derived from the first and most concrete directive that was provided to support the confidentiality of individual information, the Bill of Rights to the U.S. Constitution (1791). The Fourth Amendment explicitly guarantees individual protection against unreasonable search and seizure. It does not offer an explicit guarantee of a right to privacy. However there are several laws that derive directly from that Amendment:

The Freedom of Information Act—The Freedom of Information Act (FOIA) (5 U.S.C. 552 Public Law 890554) enacted in 1966, actually provides the first protection for the electronic age. Prior to the passage of FOIA, the burden of proof was placed on the individual to locate and request to see records the government might have about them. Under FOIA, the burden of proof shifted to the government and the "need to know" standard was replaced with a "right to know." Specifically, the FOIA guarantees access to the documents that are held by agencies in the executive branch including all cabinet departments. FOIA does not apply to elected federal officials, federal judiciary, private companies, individuals who receive federal contracts or grants, tax exempt organizations, and state and local governments. FOIA requires that Federal agencies must provide the fullest possible disclosure of information to the public. Included in the act are standards for determining which records should be made available for public inspection, and which records may be withheld from disclosure and administrative and judicial remedies for those denied access to records. The records available for request under the FOIA include all records of a Federal agency. In 1986, amendments to FOIA gave agencies some authority to deny access to a record or refuse to confirm its existence. There are three specific instances where this applies. First, there are the records that might interfere with an active law enforcement investigation. Records may be denied if they are from confidential informants, and finally, records that pertain to foreign intelligence can be withheld.

The Privacy Act—In 1974 Public Law 93-579, better known as the "Privacy Act" defined the rights of individuals with respect to the computerized information that is kept about them. This act is the first instance of the omnibus regulation of electronic information. The Privacy Act requires the U.S. government to safeguard the integrity, confidentiality, and availability of all of the personal data that is processed by federal agency computer systems. The Privacy Act essentially ensures that this collection, maintenance, use, or dissemination is for a necessary and lawful purpose. It gives individual citizens the right to see what computerized records are kept about them as well as to modify that information if it is not correct. It prevents personal records

from being used for purposes other than those that were intended or where the owner did not provide express consent. All federal agencies and by implication any agency engaged in interstate commerce, such as an ISP, are subject to damages from willful or intentional acts that violate an individual's rights under this Act.

The Computer Fraud and Abuse Act—The first real law that addressed crimes committed using a computer is Public-Law 99-474, the Computer Fraud and Abuse Act (1986). This act establishes through federal mandate that a person is in criminal violation of the law who knowingly accesses a computer without proper authorization, exceeds their permitted access, uses that access to cause a loss greater than $1,000, and performs an act—such as launching a denial-of-service attack—that prevents other authorized users from using their computers. The Fraud and Abuse Act further prohibits unauthorized or fraudulent access to government computers. It specifically prohibits access with intent to defraud and it prohibits intentional trespassing, which is the legal term for "hacking." The act is restricted to "federal interest computers," which is not as narrow as it might seem. It applies not only to computers that are owned by the government or used by the government. It also applies to computers that access federal data or computers that are located in two or more states, e.g., connected via the Internet. This provision extends federal jurisdiction into every nook and cranny of the private sector. It specifically applies to computers utilized by federally insured financial institutions and makes it a misdemeanor to post stolen passwords or obtain or even look at the data in a computer that fits that provision, such as in the case of banks.

In 1990, Robert T. Morris was the first person tried for the first true cyber crime under this act. As an undergraduate student at Cornell University, Morris wrote a self-replicating worm that spread itself from computer to computer. The Supreme Court upheld Morris's conviction by deciding that the wording of Public Law 99-474 was sufficient to define the facts of unauthorized access. Their view was that the defendant had demonstrated sufficient intent to injure to justify his conviction under the Law of authorization to access

provisions. However, as currently worded the law leaves no distinction between people who use computers for recreational hacking, versus those who use it for crime or terrorism, so there will be amendments as the precedents evolve.

The USA Patriot Act—In response to the September 11th Terrorist Attack in New York, a number of legislative actions were taken that serve to remove many of the legal protections we have discussed. Specifically, the awkwardly titled "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism," commonly known as the USA Patriot Act, extends law enforcement and intelligence agency authority to monitor private communication and access the personal information of individuals.

Public Law 100-235—This act may be cited as the "Computer Security Act of 1987" and was enacted to provide for a computer standards program and to govern classified information (P-L100-235). Its focus is on ensuring the security and privacy of the information that is contained in federal computer systems. In that respect, this due diligence law has been the most influential of all of the laws that have dictated the information assurance agenda of the federal government. Public Law 100-235 applies to all federal agencies, state agencies, and all government contractors. The act requires a central authority to develop guidelines for protecting unclassified, but sensitive information stored in government computers. The purpose is to prevent loss or unauthorized modification and disclosure of public information, as well as prevent computer fraud and abuse. It mandates that every U.S. government computer system that processes sensitive information must have a customized security plan. In conjunction with that stipulation every federal agency is required to formulate such a security plan and each agency is required to provide training for its employees on the threats and vulnerabilities of its computer systems. In service of this aim, federal agencies are required to establish security plans for systems that might handle sensitive information.

Additionally, those agencies are required to establish periodic security awareness, training, and education (AT&E) programs for every

worker who might be involved in the management, use, or operation of systems that contain sensitive information. Specifically, that training must address all relevant security threats and vulnerabilities and communicate the accepted security practices. Finally, this act locates the responsibility for controlling the computer security standards, guidelines and training programs that are issued for all federal government computer systems with NIST.

The Federal Information Security Management Act (FISMA)—The law that extends the recommendations of 100-235 into the entire federal space. Title "44 U.S.C. § 3541," better known under the short title as the Federal Information Security Management Act of 2002, is a United States federal law enacted to strengthen information security and to provide a comprehensive framework for ensuring the effectiveness of information security controls. The act recognizes the importance of information security to the economic and national security interests of the United States. The act requires each federal agency to develop, document, and implement an agency-wide program for securing information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source (FISMA).

FISMA emphasizes a "risk-based policy for cost-effective security." It requires agency program officials, chief information officers, and inspectors general (IGs) to conduct annual reviews of the agency's information security program and report the results to the Office of Management and Budget (OMB). OMB uses this data to assist in its oversight responsibilities and to prepare this annual report to Congress on agency compliance with the act. FISMA assigns specific responsibilities to federal agencies, the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) in order to strengthen information system security. In particular, FISMA requires the head of each agency to implement policies and procedures to cost-effectively reduce information technology security risks to an acceptable level. According to FISMA, the term "information security" means protecting information and information

systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability.

In accordance with FISMA, NIST is responsible for developing the appropriate standards, guidelines, and associated methods and techniques in order to provide acceptable information security for all agency operations. NIST works closely with federal agencies to improve their understanding and implementation of FISMA. NIST publishes standards and guidelines that provide the foundation for strong information security programs at agencies. NIST develops standards, metrics, tests, and validation programs to promote, measure, and validate the security in information systems and services.

FISMA defines a framework for managing information security. That framework must be followed for all information systems used or operated by a U.S. federal government agency or by a contractor or other organization on behalf of a federal agency. This framework is further defined by the standards and guidelines developed by NIST. FISMA requires that agencies have in place an information systems inventory. Organizations must meet the minimum security requirements by selecting the appropriate security controls and assurance requirements as described in NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems."

Skills Needed by the Cybersecurity Workforce

It goes without saying that the typical skills needed to ensure all of the relevant areas of threat will be rooted in several bodies of knowledge. Nevertheless, the first thing to keep in mind when looking at the requisite knowledge is that cybersecurity is an emerging discipline. In that respect, according to a report from the National Academies of Science, it is not exactly clear what the field comprises (Burley, 2015). The lack of a hard-and-fast definition is understandable since 15 years ago cybersecurity was an interesting sideshow rather than a main tent attraction. From a practice standpoint, cybersecurity is fragmented into

two major camps. First, there is the group that takes a computer security focus. This is primarily a governmental and military perspective. They contend that their only role is to protect information from electronic attacks and that other types of practitioners are responsible for the behavioral and physical aspects of information protection. Then there is a larger group with more of a general business and higher education orientation. This group contends that the wide-spectrum attacks, which are characteristic of today's cyber threats, demand a consolidated approach to the problem. The term "holistic" has been used to describe this approach. The holistic approach embraces a much broader set of disciplines.

If comprehensive protection is the goal, holistic study of cybersecurity could embrace a range of content including: Business, Accounting, Information Systems and Software Engineering, Law and Forensics, Computer Science and Networking. It even includes content from such logically unrelated areas as Military Science, Education, and Ethics. Business contributes the procedural aspects of security policy formulation, security infrastructure development, continuity planning, personnel management, privilege setting and access control, and contract and regulatory compliance. The discipline of Accounting underwrites the audit certification of security systems and such legal requirements as Sarbanes-Oxley compliance, HIPAA compliance, banking, and compliance to the U.S. Securities and Exchange Commission regulations. The disciplines of Information Systems and Software Engineering contribute cybersecurity concepts like asset baselines and configuration management, development process security, and system and software security. Law and Forensics contributes intellectual property and copyright protection, privacy legislation, cyber law and litigation, and investigation and prosecution of crimes. Computer Science contributes all of the technical aspects of processing information in its electronic form. That includes all forms of computer security, plus all of the technical aspects of network security and cryptography. Military Science contributes such concepts as defense in depth, offensive countermeasure deployment, Infowar and OPSEC. Education adds security awareness, security training, and certification in industry and higher education security teaching and research. Even Ethics contributes essential con-

cepts like codes of conduct, business rules, and cyber rights. In every instance, each selected content element assures a specific aspect of the problem. All of them, or some subset of them, might be required to accomplish the requisite security goals of any given instance. The integrated set forms a mutually supporting system that provides the desired level of assurance. Consequently, knowledge from all of these areas can be assumed to be part of a proper cybersecurity response.

There is still much debate in the field as to whether the purely electronic view, or the holistic view of cybersecurity is correct. That point is where the National Initiative for Cybersecurity Education's (NICE) National Cybersecurity Workforce Framework (2.0) comes in. Cyberspace is complex and the field itself is rapidly evolving. That is why a single definitive specification of the knowledge, skill, and ability requirements for a well-educated cybersecurity professional is so critically important (Wilshusen & Barkakati, 2015). The National Initiative for Cybersecurity Education (NICE) developed the National Cybersecurity Workforce Framework (2.0) to underwrite a common understanding of cybersecurity work (NISTc). Its stated aim is to completely and correctly define all of the roles in the cybersecurity workforce and to provide a set of standardized terms for use in cybersecurity work. The Workforce Framework (2.0) is based on "Categories" or "Specialty Areas" within the workforce, and the requisite "Knowledge Skills and Abilities" for each specialty area. Each type of cybersecurity work is placed into one of seven overall categories. The categories serve as an overarching structure for the field and were used as an organizing construct to group similar types of work.

The intention of the Workforce Framework (2.0) is to describe cybersecurity work regardless of organizational structures, job titles, or other potentially idiosyncratic conventions. The categories aim to group related specialty areas together. The Workforce Framework (2.0) lists and defines 32 specialty areas of cybersecurity work and provides a description of each. In essence, knowledge specialty areas in a given category are typically more similar to one another than to specialty areas in other categories. Typical tasks and knowledge, skills, and abilities (KSAs) are provided within each specialty area. The Workforce Framework (2.0) also identifies common tasks and knowledge, skills,

and abilities (KSA's) associated with each specialty area. The United States Office for Personnel Management (OPM) has mandated that the NICE Cybersecurity Workforce Framework (2.0) will be used to guide the federal government and will also be made available to the private, public, and academic sectors for describing cybersecurity work and related education, training, and professional development.

The NICE Workforce Framework (2.0) comprises seven general Categories of professional roles. There are presently 32 Specialty Areas and 65 job titles in the model. The first of these Categories is Securely Provision. Securely Provision itemizes the specialty areas within the workforce that are responsible for conceptualizing, designing, and building secure information technology (IT) systems (i.e., responsible for some aspect of systems development). The next category is Operate and Maintain. Operate and Maintain comprises the specialty areas responsible for providing support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security. The next category is Protect and Defend. As the network security area of the framework, its specialty areas are responsible for identification, analysis, and mitigation of threats to internal information technology (IT) systems or networks. The fourth area is Investigate. Its specialty areas are responsible for investigation of cyber events and/or crimes of IT systems, networks, and digital evidence. Essentially this category covers the field of cyber forensics. The fifth area is Collect and Operate. Its specialty areas are responsible for specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence. The sixth area is Analyze. Its specialty areas are responsible for highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence. The final area is Oversight and Development. Specialty areas here provide leadership, management, direction, and/or development and advocacy so that individuals and organizations may effectively conduct cybersecurity work. The general consensus is that the Framework will enable all organizations to describe their cybersecurity work and workforces at a standard level of consistency, detail, and quality. It is only with this understanding that organizations can analyze and explain the factors and dynamics that influence the workforce and work requirements.

Recommendations for Cybersecurity Best Practices

As stated, there are a seemingly infinite variety of threats and a wide range of countermeasures and controls that can be implemented. Thus a single coherent approach is required to build the protection scheme. The strategy must produce a complete solution, which can then be rationally evolved to meet the changing needs of the environment. The strategy must ensure a trustworthy long-term assurance capability, which will address all likely threats, and respond appropriately to all incidents. In order to ensure the requisite degree of operational capability, the cybersecurity system must be established through a formal organization-level process. In essence, the cybersecurity solution has to be designed to merge all requisite practices and technical controls into a single coordinated approach. That approach must directly support and be traceable to all of the conditions of the assurance case, as well as objectively demonstrate trustworthiness.

All cybersecurity processes embody an established collection of common components, which are designed to work together to produce an optimum solution. The overall process can be understood and described in terms of those fundamental components and their logical interactions. Moreover, they can also be used to derive an implicit structure for the process. Genuine assurance implies that all of the elements necessary to ensure reliable protection have been created. Consequently, besides technical controls the security solution must also incorporate all relevant organizational and human factors into a total system of protection that has a logical progression of steps. That is, there is a clearly identifiable point of initiation where the cybersecurity development process begins. Subsequently, the development of the solution follows a logical path to a suitable conclusion. The figure below illustrates the sequence of the lifecycle practices needed to ensure a comprehensive cybersecurity solution.

As shown in Figure 1.1, the first step in the cybersecurity lifecycle process is asset identification and the goal is to identify all of the components of the information asset, label them, and then baseline them. Once that is accomplished, the next step, risk assessment, is to identify all of the relevant threats, vulnerabilities and weaknesses that influence that baseline. The vulnerabilities and risks are then specified

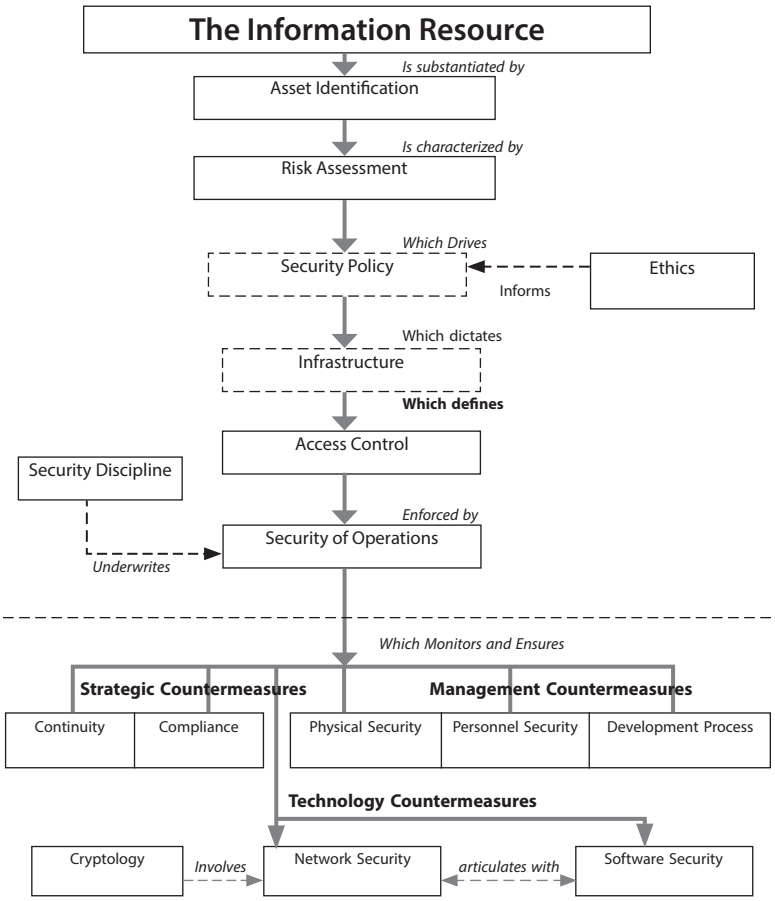

Figure 1.1. The Cybersecurity Lifecycle Figure *(Courtesy of the authors)*

and prioritized, which then drives the continuous evolution of a logical and substantive security policy and control framework. This structure is necessary to establish and maintain a consistent, applied process. The next step is to develop a set of policies/controls that accurately address the known situations within a proper, ethical frame of reference. From the general guideline policies, security controls are then

developed into a complete, detailed and appropriate set of practices that comprise the visible aspects of the security infrastructure for the given situation.

The security controls and practices are implemented and overseen by the security of operations function. That function is the day-to-day management element of the process. The aim of the security of operations is to ensure that all policy and procedural requirements are met and that all countermeasures are correctly installed and operating as intended. The countermeasures that will be deployed will depend on the threat environment. The specific threats that need to be defended against, previously identified in the risk assessment report, and the specific protection strategy that is chosen, are captured in the security control infrastructure that is developed as a result of that analysis. The resulting countermeasures include all of the technological and managerial countermeasures deemed necessary to implement the various functional areas of protection.

The security control set represents the selected best practices that are deployed to meet the various protection needs implicit in the particular circumstance. The detailed procedures for maintaining acceptable protection in each of the functional areas are itemized in the assurance plans for each area and operationally managed. And they are subject to any necessary revisions that might pass through the prior domains.

The process for developing countermeasures is fairly standard and the following is a more detailed look at the process:

Asset Identification—Knowing what you need to protect is a precondition of any security process. So first we have to look at asset identification. Cybersecurity requires a precise identification of every item of value that will be secured, such as people, data/information, software, hardware, and the infrastructure. The exact form of the items that will be placed under security management must be explicitly defined and documented. This activity requires an inventory of the resources to differentiate them, explicitly describe their contents, and then to assess value to each asset. The process of identification and labeling creates a tangible picture of the exact form of all assets. That picture

then serves as the specific point of reference for the deployment and management of the security function and is generally called a baseline.

Risk Assessment—Next, we need to assess the risks to each asset. The analysis phase includes the identification and examination of all possible threats as well as the prioritization of the harm. It is necessary to have that prioritization because it is impossible to protect against all threats due to the cost and time involved. Thus a tradeoff has to be performed. This activity is always based on the degree of estimated risk. The risk assessment can be either formal or informal, but the idea is to identify all realistic weaknesses facing the organization. These are assessed and classified in the form of a two-dimensional table. That is because threat types are either physical or virtual and they can only originate from internal or external sources. The table can be used to estimate expenses and begin to identify the possible security controls needed.

All risks are ranked and then prioritized. The aim is to counter the threats with the greatest likelihood of harm, taking into consideration the resources available. There are several risk control strategies such as defense-in-depth, transferrable, and mitigation. The defense-in-depth approach attempts to ensure against threats that absolutely must be defended. The threats that might cause significant harm are defended on a sliding scale from most important to least important. At the point where resources are not available for further protection, a decision is made to either accept the risk or obtain more resources. The transferrable approach attempts to shift risk to other assets by purchasing insurance, outsourcing to strategic partners, or changing the way the organizations offers its products and services. The mitigation approach attempts to reduce the impact of a security breach through thorough planning, testing, and preparation.

Policy—Once the risks are identified it is necessary to define policies for how they will be countered. Policies must be integrated in order to establish the framework of the response. They are essential elements of security because they establish the overall form and direction of the response. The practical outcome of the asset identification and control baseline formulation process is a functioning security system.

Procedure—The role of policies are to provide coordination and general guidance. The form of the response is dictated by the concrete procedures and resultant practices that implement each procedure. The complete set of procedures is called the security infrastructure. The policies and procedures dictate precisely HOW the assurance controls will interact within the cybersecurity scheme. The application of the required controls for each information item must be spelled out in the form of itemized work practices, which are referenced to the relevant policies and procedures. This specific linkage is necessary in order to avoid any potential misunderstanding in the subsequent practical use. Steps that need to be taken during this process include the specification of work practices to dictate the sequence and timing of control usage; specific monitoring practices; establishing accountabilities, documentation, and reporting; and problem resolution responsibilities.

Security of Operations—The security of operations is a critical part of the information assurance lifecycle. Its role is to ensure the integrity and performance of the rest of the organization's security processes. It confirms that policies and procedures are consistently followed. It monitors and evaluates day-to-day execution of the continuity, compliance, physical security, and personnel security processes. It establishes that all technical countermeasures are in place and operating properly.

When problems are detected, the security of operations is ultimately responsible for coordinating the right corrective action response. Without security of operations, the organization would not be able to guarantee the long-term viability of its information assurance capabilities. The security of operations process involves such representative actions as ensuring that current operating procedures are properly aligned with security policies, monitoring the performance of security duties to confirm that they correspond to proper procedure, and defining standard operational testing strategies to validate that security continues to operate properly.

As the name implies, security of operations is less involved with strategy than it is with underwriting dependable day-to-day performance. Security of operations accomplishes organizational performance by ensuring that security practices always meet the security goals.

Every organization has security goals. Those goals must be satisfied in order for the organization to be secure. However, the overall security environment is always changing and so the goals change accordingly. Factors that can affect this include changes in the people who use the system and their motivations, external systems interconnected with the organization's systems, the type and sensitivity of data flowing to or from the organization's system, the type and way the organization does business, the rigor of the security objectives, and the chosen organizational risk model/risk tolerance approach.

If a particular practice no longer fulfills a given security goal, then the organization has to undertake a risk assessment process to decide whether to change the practice or the requirement. Changes to requirements might include the reclassification of information to a different sensitivity level or altering the access rules for a given facility. Factors that might lead to changing the requirement, rather than practice, include the availability of time and resources and the existence of feasible alternatives.

In every case however, the logical outcome is that security requirements must always align with security practice. In this respect, the role of security of operations is to maintain a correct alignment between the organization's security goals and its security practices. Security of operations is responsible for monitoring the execution of each of the other processes in order to ensure that alignment. The focus of that monitoring activity is in the detection of meaningful deviations from correct practice. Typically, this is accomplished by identifying and recording problems as they occur, analyzing each problem to develop effective countermeasures, taking the appropriate corrective, adaptive, perfective or preventive action, and validating the integrity of the change. Furthermore, the security of operations function routinely reviews, inspects, tests and audits the performance of the elements that constitute the overall security response. Where problems are encountered the security of operations is the function that is responsible for coordinating the problem resolution.

As such, security of operations and intrusion detection might be considered to be two seamless aspects of the same larger purpose, which is to ensure that every conceivable threat is identified and

appropriately responded to. The commonsense goal of security of operations is to anticipate all likely security events and have a pre-defined response in place. Which leads to the final aspect of the security of operations function: ensuring a timely response. Responses can be either proactive or reactive. Proactive activities include the identification of threats and vulnerabilities, the creation, assessment, and optimization of security solutions (within a generalized security architecture), the implementation of controls to protect the software and the information that it processes, and the threat response. Reactive activities include ensuring timely threat response and the detection and reaction to external or internal intrusions or security violations.

Human Factors—Human Factors determine how the security response is implemented. In essence these "intangible" factors are what makes each security system unique and they inform the shape of the solution. Threats to corporate information arise at various levels and appear in a variety of ways. These range from penetrations of the network by technically sophisticated "hackers," all the way down to petty thefts perpetrated by people who knowingly, or even unknowingly, take something of value. As a consequence, people are easily the weakest link in the system due to their behavior and cannot be left to chance. It has to be addressed by a tangible set of practical countermeasures designed to eliminate the human factor as the chief vulnerability.

It is difficult to be assured that the people involved in the day-to-day process of handling information will think to do everything necessary to protect it. That is the reason for procedure, but procedures have to be consistently followed in order to be effective. Therefore the successful execution of the process entails human elements such as understanding and acceptance. The annual Privacy Clearinghouse survey has consistently identified human factors as the primary point of failure in the overall security process (PRC). Human factors influence security performance because they dictate how rigorously rules are followed and how consistently prescribed actions are taken. As a result, the human aspect should never be ignored in the design of a competent process (Smith, 2012).

Salzer and Schroeder (1974) identified eight principles for implementing and maintaining a disciplined system of rules of behavior for all participants. The following is a list of the 8 principles:

1. Economy of mechanism—Keep it simple.
2. Fail-safe defaults—The authentication principle. Base access decision on whitelists, not blacklists. Assign trust before allowing access.
3. Complete mediation—The authorization principle. All access to all system objects has to be authorized.
4. Open design—Base access on separate authentication tokens; what you know, what you have and who you are, or some combination of those three things.
5. Separation of privilege—No single person should control a process. In essence it should take two people or more to authorize an action.
6. Least privilege—"Need to know." A user should have no greater access than required to do their job.
7. Least common mechanism—Modularity principle. Keep all authorized operations partitioned in a way that each individual user can only operate in their assigned areas of authorization.
8. Psychological acceptability—Ease of use principle. People will not follow procedure if it is too difficult, for instance an over complex password

Future Trends in the Information Technology (IT) Sector

With technology, any thoughts about the future are pure speculation. For instance, who could have imagined only 20 years ago that we would be where we are with securing the global information grid (GIG). Just ten years ago cybersecurity was still something of an arcane study. In 2004, there were 40 NSA Centers of Academic Excellence

in Information Assurance Education (CAE/IAE). Now there are 192. So predicting the future is a perilous venture. Nevertheless, there are probably five areas that have the likeliest growth potential.

First and foremost, there is Mobile Security. Information and communications technologies have become ubiquitous today. People order pizza and do their banking using hand-held tablets, or their mobile smartphones. As a result, they keep infinite amounts of very personal and potentially sensitive data in their pockets or purse. All of those devices are subject to hijacking and the number of celebrity incidents alone should demonstrate the scope of the problem. Moreover, there is no sign that mobile computing will become less omnipresent over time. People just like the freedom to surf the Web on their phone. Because of the proliferation of those devices it is speculated that over time, mobile security might become a separate profession from traditional cybersecurity, with its own knowledge skill and ability requirements.

After the Internet itself, the single most influential business innovation is cloud computing. Thus it is inevitable that cloud security efforts will continue to grow. One issue with storing data in the cloud is that businesses lose control over the data that is stored there. Because of the economies and ease of operation of the cloud, most businesses accept the risk. However, the level of trust that is necessary between the client and the provider has to be absolute, otherwise the risk of loss or disclosure begins to outweigh the economies of scale. Cloud security is necessarily nebulous, no pun intended. The data itself is stored on massive server farms and it is controlled and stored by the portals that receive and transmit the information. Because those portals are automated even the operators themselves might not know exactly what is happening to an individual user's information. Since the technological capability has arrived long before we have a mature idea of how to handle it, cloud computing will no doubt undergo considerable refinement in the cybersecurity research and development community. In addition, the efforts to both illegally obtain as well as protect cloud applications will no doubt continue to grow.

Acquisition and supply chain risk management are related areas that have come to the forefront as a result of the globalization of the software business (Shoemaker & Mead, 2013). Due to the time and

cost advantages it is far preferable to obtain a system as a product, rather than develop it as was necessary 20 years ago. That product is called Commercial Off-the-Shelf or COTS. Because of the rise of global outsourcing most companies integrate code that has been developed in other parts of the world into their products. And given the complexity of those products the actual development and integration often takes place along a supply chain that hops from country to country. Needless to say, any security breakdown along that chain can lead to the insertion of back doors, and other bits of malware in a finished product. What is worse, because the supply chain extends from contractors to subcontractors down several levels, it is likely that the customer will not know who actually created their base code. "Unknown authors of source code" is unacceptable with a commercial product. It is even less acceptable with government weapons systems and other National Security applications. Thus, supply chain risk management and secure acquisition is developing as a co-equal branch of the entire cybersecurity profession.

The Deep Web and the Dark Web are unexplored territories for the cybersecurity profession. They are going to be an emerging issue because the visible Internet is only the tip of the iceberg. The Deep Web has gotten more visibility than the Dark Web because the media has discovered it. The Deep Web is nothing more than unindexed locations (Russell, 2005). There are various reasons why the spiders at Google and other engines are unable to see those sites, and there are 500 invisible sites in the Deep Web, for every visible location on the visible Internet. Therefore, a lot of clandestine things could be happening in the Deep Web, including crime and espionage.

The Dark Web is based around The Onion Routing (TOR) program, which is made up of projects to research, design, build, and analyze anonymous communications systems. If you want to do something illegal, TOR is the place to do it. TOR is one stop shopping for anonymous, untraceable Internet activity. Using the Dark Web people can buy illegal drugs at sites like "The Silk Road" and even order up a hit man (yes, they advertise in the Dark Web). Hence, the Dark Web is like the bad side of town. Generally, nobody goes there unless

they are up to no good. And as a consequence, law enforcement and intelligence agencies are beginning to view the Dark Web as a place of interest for future investigation.

Supervisory Control and Data Acquisition, SCADA, is on the other end of the scale from Supply Chain Risk Management. Most of the automatic operations that we simply take for granted within our entire infrastructure are controlled by programmed logic devices. Those devices are like the insect world, they might be small and they may be simple but they are everywhere around us. And every aspect of the U.S. infrastructure depends on them. The problem is that these devices are too simple to have ANY security built into them and thus they are completely open to exploitation. Additionally these logic devices are controlled by a Supervisory Control and Data Acquisition (SCADA) system that utilizes networks that could cause them to be subject to exploitation (Shah, 2014). The specter of an adversary being able to control critical infrastructure systems such as power, oil and gas, or banking through a breach of a SCADA system raises issues of true national importance (Santos, Haimes, & Lian, 2007). Yet SCADA security is a small and ignored subset of the field. If a tragedy results from that kind of exploitation, SCADA will become a much more important issue and an area of potential massive growth in the future.

Social Engineering is not electronic, nor does it actually involve computers. Nevertheless there are some estimates that the majority of the loss and harm to electronic information originates in the behavioral universe. The term "social engineering" has been around for a long time in the social sciences but lately it has come to apply directly to cybersecurity. Social engineering is a non-technical method that hackers use and involves tricking people into performing unauthorized acts using a computer (Tetri & Vuorinen, 2013). In simple terms, this con-game poses one of the greatest threats to organizations. Since people are the target and there are an infinite number of ways that they can be manipulated, there is no specific remedy. The general solution is to provide sufficient awareness, training, and education to ensure a digitally literate professional community—one that can recognize even the most sophisticated cons. That effort is currently

not coordinated enough to be effective but it will have to be in the future since social engineering is very profitable. There is an estimate that over half of the organizations in America annually suffer social engineering attacks and that the losses from those attacks amount to over $100,000 per incident (Schwarz, 2011).

There exist many other areas where there is potential for huge change. Malware is always a concern, which has been the case since the beginning of the Internet. Social Media as a method of attack and exploitation is a new phenomenon, but given its popularity that area is also likely to become a hot topic in the future. Finally, there is the Bring Your Own Device (BYOD) movement that has only recently taken off but could become the biggest security issue of all for businesses in the next five years. None or all of this may happen. It depends on where the technology takes us. But it is certain that cybersecurity will always be an issue for our future.

Sources of Further Information

Department of Homeland Security, Build Security In, https://buildsecurityin.us-cert.gov/

National Initiative for Cybersecurity Careers and Studies, http://niccs.us-cert.gov/

The National Initiative for Cybersecurity Education, http://csrc.nist.gov/nice/

Software Engineering Institute, http://www.sei.cmu.edu/

Colloquium for Information Systems Security Education, http://www.cisse.info/

Open Web Application Security Project: https://www.owasp.org/index.php/Main_Page

Common Weakness Enumeration, http://cwe.mitre.org/

References

Bissell, K. (2013, March). A strategic approach to cybersecurity. *Financial Executive*, 29(2).

Burley, D. L., Eisenberg, J., & Goodman, S. E. (2014, February). Would cybersecurity professionalization help address the cybersecurity crisis? *Communications of the ACM,* 57(2), 24–27.

Computer Fraud and Abuse Act of 1986. (1986). Public Law 99.474.

Computer Security Act of 1987. (1988, January). Public Law No. 100-235, H.R. 145.

FISMA-Federal Information Security Management Act. (2002). Chapter 35 of title 44 United States Code, 48–63.

Freedom of Information Act. (Amended 2014). Public Law 5 U.S.C. § 552, 1–19.

GAO Report to Congressional Requesters, United States Government Accountability Office. (2012, March). IT supply chain: National security-related agencies need to better address risks, 1–45.

Harknett, R. J., & Stever, J. A. (2011). The new policy world of cybersecurity. *Public Administration Review,* 71(3), 455–460.

International Standards Organization (ISO). (2012). ISO 27000, Information technology—security techniques—information security management systems—overview and vocabulary.

Martin, R. A. (Ed.). (n.d.). Common weakness enumeration. Mitre Corporation.

Moran, T. H. (2013). Dealing with cybersecurity threats posed by globalised IT suppliers. *Policy*, 29(3), 10–14.

NIST. (2006a). Federal Information Processing Standard FIPS PUB 200—Minimum security requirements for federal information and information systems. National Institute of Standards and Technology, 1–11.

NIST. (2013b). NIST Special Publication 800-53, Rev. ed. 4, Security and privacy controls for federal information systems and organizations. National Institute of Standards and Technology, 1–462.

NIST. (2014c). The national cybersecurity workforce framework 2.0. National Institute of Standards and Technology.

Pfleeger, S. L., & Rue, R. (2008). Cybersecurity economic issues: Clearing the path to good practice. 25(1), 35–42.

PRC. (2013, December 31). Chronology of data breaches security breaches 2005–present. Privacy Rights Clearinghouse.

Privacy Act of 1974. (1974). Public Law 93-579, as codified at 5 U.S.C. 552a, 1–27.

Russell, K. (2005, December 19). DeepWeb. *Computerworld,* 39(51), (p. 28).

Saltzer, J. H., & Schroeder, M. D. (1974). The protection of information in computer systems. *Communications of the ACM*. 17(7).

Santos, J. R., Haimes, Y. Y., & Lian, C. (2007, October). A framework for linking cybersecurity metrics to the modeling of macroeconimic interdependencies. *Risk Analysis: An International Journal,* 27(5), 1283–1297.

Shah, G. C. (2014, February). What managers should know about pipeline SCADA cybersecurity. *Pipeline & Gas Journal*, 241(2), 62–63.

Shoemaker, D., & Mead, N. (2013). Building a body of knowledge for ICT supply chain risk management. *Crosstalk: The Journal of Defense Software Engineering*, 24–28.

Shoemaker, D., & Kennedy, D. B. (2009). Criminal profiling and cybercriminal investigations, pp. 456–476 in M. Pittaro & F. Schmalleger (Eds.) *Crimes of the Internet*, Upper Saddle NY: Prentice-Hall.

Smith, R. E., (2012). A contemporary look at Saltzer and Schroeder's 1975 design principles. *IEEE Security and Privacy* 6(10), 20–25.

Suby, M. (2013). The 2013 $(ISC)^2$ Global Information Security Workforces study. International Information System Security Certification Consortium (ISC^2), Frost and Sullivan, 1–26.

Tetri, P., & Vuorinen, J. (2013). Dissecting social engineering. *Behaviour & Information Technology*, 32(10), 1014–1023.

Toecker, M. (2014). Generation cybersecurity: What you should know, and be doing about it. *Power*, 40–45.

Wilshushen, G. C., & Barkakati, N. (2013, February). Cybersecurity: National strategy, roles, and responsibilities need to be better defined and more effectively implemented. GAO Reports, 1–104.