The Cybersecurity Body of Knowledge

CRC Press
Taylor & Francis Group
52 Vanderbilt Avenue,
New York, NY 10017

Printed on acid-free paper

International Standard Book Number-13: 978-0-367-90094-6 (Hardback)

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Contents

Foreword 1

I have great pleasure in writing this foreword. I have worked with Dan, Anne, and Ken over the past six years as this amazing team has written six books for my book collection initiative. Their newest effort, *The Cybersecurity Body of Knowledge: The ACM/IEEE/AIS/IFIP Recommendations for a Complete Curriculum in Cybersecurity,* brings together a comprehensive understanding of cybersecurity and should be on the book shelf of every professor, student, and practitioner.

Right now, the study of cybersecurity is pretty much in the eye of the beholder. This is the case because the number of interpretations about what ought to be taught is only limited by the number of personal agendas out there in the field.

Through discussion with the team, I've learned that every well-established discipline of scholarship and practice has gone through the process of research, extensive discussions, formation of communities of practice, and thought leadership to continually build the body of knowledge. Over time, diverse voices put forth ideas, concepts, theories, and empirical evidence to advance the thinking, and in every discipline, there comes a time when thought leadership establishes generally accepted standards based on a comprehensive view of the body of knowledge.

I believe that time has come for the discipline of cybersecurity.

Beginning with a narrow focus on computer security, the discipline has advanced tremendously and has accurately become known as a fundamentally computing-based discipline that involves people, information, technology, and processes. Additionally, as the threat environment continues to expand, due to the expanse of global cyber infrastructure, the interdisciplinary nature of the field includes aspects of ethics, law, risk management, human factors, and policy. The growing need to protect not just corporate information and intellectual property but also to maintain national security has created a demand for specialists, across a range of work roles, with the knowledge of the complexities of holistically assuring the security of systems. A vision of proficiency in cybersecurity that aligns with industry needs and involves a broad global audience of stakeholders was needed to provide stability and an understanding of the boundaries of the discipline.

The formation of the CSEC2017 Joint Task Force – involving four major international computing societies: the Association of Computing Machinery (ACM), the IEEE Computer Society (IEEE CS), the Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC), and the International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8) – came together to publish the single commonly accepted guidelines for cybersecurity curriculum (The CSEC2017 Report). The CSEC2017 Report has produced a thought model and structure in which the comprehensive discipline of cybersecurity can be understood. With this understanding, development within academic institutions and industry can prepare a wide range of programs that are

grounded in fundamental principles.

This book explains the process by which the CSEC2017 was formulated, its pedigree, and then it discusses the knowledge units of each of the eight knowledge area categories of the field in detail. Upon reading this book, the reader will understand the knowledge that is required as well as a basic understanding of the application and purpose of each of these myriad elements.

I have studied the various chapters and believe the seamless flow of the content will be beneficial to all readers. The extensive use of visuals greatly improves the readability as well as supports a better understanding of the extensive number of knowledge topics that are involved. While knowledge knows no end, dissemination and sharing of knowledge are critical in today's world. I believe this book will help form the foundation of a comprehensive and generally accepted cybersecurity body of knowledge and I congratulate the team on their work and their amazing result.

Dan Swanson

Series Editor

Foreword 2

Cybersecurity is professionalizing. As a field, it has spawned from technical disciplines where it is an increasingly difficult fit, given its increasingly interdisciplinary nature. What started as a one-size-fits-all subject, about mitigating vulnerabilities in information systems, is now expected to cover the range of topics that a Chief Information Security Officer must consider when building an approach to keeping information safe within an organization. This not only includes the technical tools but also things such as policy, procedures, awareness training, audit, compliance, law, and privacy. These subjects clearly go beyond computer science or electrical engineering where students learn to build and apply cybersecurity system components.

Add to this challenge the fact that cybersecurity is evolving quickly. No sooner is a book published than it begins to become out of date! What a challenge for academics and practitioners alike to stay current! And if cybersecurity is becoming a profession like medicine or law, how difficult it becomes to ensure that employers in different parts of the country know what knowledge is in the minds of the cybersecurity expertise they hire. These are employees they are entrusting with the very life blood of their organizations, their information. There is a reason practitioners refer to the "crown jewels" of the company when they identify their most sensitive and valuable data.

With Snowden's and the Manning's raising awareness of how vulnerable an organization's information can be, how big the impacts if compromised, we need to ensure that those we hire to protect it have the knowledge, experience, integrity, and maturity to warrant trust. Hence, the effort to professionalize the field. We're seeing the emergence of codes of conduct, internship programs, certification testing, and standard curricula—all hallmarks of a profession.

Educational standards are at the very heart of any professional discipline. We need to know what those we hire know. Using medicine as an example, we have comfort that no matter what medical school a doctor attends, the basic curriculum is the same and we have board exams and accreditations for verification. Likewise, we need to have the same for cybersecurity, a practice that, if not performed well, could cripple infrastructure, bring down cities, and even cause deaths in the case of medical devices that are increasingly relied upon, yet are exposed online.

My colleagues Daniel Shoemaker, Anne Kohnke, and Ken Sigler have been working on standardization of cybersecurity curriculum for years – first in support of the NSA's efforts to specify what they need in a cybersecurity professional through their NIETP organization which created, working with NIST, the beginnings of educational standards and then through the various evolutions as DHS, professional organizations, certifications have made their contributions.

As the ACM has stepped up to creating cybersecurity education guidelines that invite other countries to help define them, it's time to acknowledge the development

of what is becoming a set of educational standards that cybersecurity professionals around the world are acknowledging. With their book, the authors are presenting the case for educational standards as an important part of the emerging profession of cybersecurity.

I remember not too long ago when an HR executive from a large company in my region expressed frustration that advertising for cybersecurity expertise was not enough. You need to know what subdiscipline candidates know and what knowledge base they have in their minds so you can hire appropriately. Since that conversation, NIST/NICE, NSA, DHS, and ACM have wrestled with defining the field. The author's contribution is to synthesize this history and make the case for reliable educational standards that are the foundation of any profession.

Knowing the authors as I do, I can think of no others who could better make this case and also identify the appropriate time – now – to do so. This is an important contribution to the evolution of the cybersecurity profession to the next step – a profession like any other.

This is an exciting time to be in this field. I thank the authors for their efforts.

Barbara Endicott-Popovsky, PhD
Professor and Executive Director,
Center for Information Assurance and Cybersecurity
University of Washington;
Editor in Chief,
Colloquium for Information Systems Security Educators (CISSE) Journal

Author Biographies

Daniel Shoemaker, PhD, is full professor, senior research scientist, and program director at the University of Detroit Mercy's Center for Cyber Security and Intelligence Studies. Dan is a former chair of the Cybersecurity & Information Systems Department and has authored numerous books and journal articles focused on cybersecurity.

Anne Kohnke, PhD, is an associate professor of cybersecurity and the principle investigator of the Center for Academic Excellence in Cyber Defense at the University of Detroit Mercy. Anne's research is focused in cybersecurity, risk management, threat modeling, and mitigating attack vectors.

Ken Sigler is a faculty member of the Computer Information Systems (CIS) program at the Auburn Hills Campus of Oakland Community College in Michigan. Ken's research is in the areas of software management, software assurance, and cybersecurity.

Introduction

The Vital Need for Common Agreement

Every profession is built around formal agreement about the underlying knowledge of the field. This agreement serves as the point of departure for building an academic discipline. In the case of the discipline of cybersecurity, there has never been a definitive, commonly accepted standard of the critical elements of the field. The purpose of the CSEC2017 Report (referred to as CSEC2017 for the remainder of the book) is to provide an authoritative standard.

The CSEC2017 is built around the assumption that there is a responsibility to specifically articulate what constitutes the field of cybersecurity. The goal of the CSEC2017 is to detail the communal knowledge areas and their constituent knowledge elements. In service of this, the CSEC2017 states and clarifies the separate educational elements of cybersecurity and their interrelationships to each other in professional practice. Each individual knowledge area is different in its focus and aims. Therefore, these disparate knowledge requirements need to be integrated into a single strategic infrastructure that amounts to a comprehensive definition of the field. The value of a single unified definition is that it provides the depth of understanding necessary to ensure complete, in-depth solutions.

CSEC2017 focuses on the definition of a set of standard knowledge elements rather than the usual teaching and learning issues. In essence, the CSEC 2017 provides a complete conceptual structure containing every knowledge element that is considered to be germane to the study of cybersecurity. The CSEC2017 Report essentially documents and interrelates all of the necessary learning elements into a single common definition of the discipline cybersecurity and is one of the two groundbreaking aspects of this project. The other is that CSEC2017 provides a comprehensive roadmap for teaching and learning holistic cybersecurity.

The latter is important because the lack of a common understanding of the ways in which the diverse elements of the field fit together is one of the major stumbling blocks in building coherent responses to threats. Consequently, the synthesis of the details of the cybersecurity process into a single unified understanding is an invaluable asset for cybersecurity educators.

Defining the Elements of the Field of Cybersecurity: What is CSEC2017?

The CSEC2017 Joint Task Force on Cybersecurity Education (JTF) originated in September 2015 (CSEC-JTF, 2017). The CSEC2017 mission was twofold, "To initiate the processes for (1) developing undergraduate curricular guidance and (2) establish a case for the accreditation of educational programs in the cyber sciences." (CSEC, 2017, p. 10). The recommendations in the report represent fully sanctioned, all-inclusive guidelines about the content and structure of a cybersecurity curriculum. It must be

understood that these recommendations are a single conceptual framework for the field. The CSEC2017 document does NOT specify a single monolithic approach, nor is it prescriptive. Instead, the CSEC2017 body of knowledge is meant to be used either completely or in part to develop relevant courses and to modify a broad range of existing programs or course concentrations (CSEC, 2017).

The CSEC2017 delineates the boundaries of the discipline and outlines key dimensions of the curricular structure of the study of cybersecurity. Its aim is, "To develop curricular guidance that is comprehensive enough to support a wide range of program types and to develop curricular guidance that is grounded in fundamental principles that provide stability" (CSEC-JTF, 2017, p. 11). As defined in the CSEC2017, there are eight generic knowledge areas. Taken as a whole, these distinctive areas constitute a common definition of the discipline as well as the learning elements that should be involved in the delivery of an acceptable cybersecurity learning experience.

Organization of the Text

The reader will see how to create a comprehensive cybersecurity teaching program, one that embodies the commonly recognized knowledge elements deemed essential to the field. This book will explain how each of these elements fit together.

The members of the Joint Task Force of major international computing societies identified eight knowledge areas that represent the comprehensive body of knowledge for cybersecurity education (CSEC, 2017). As with any complex design process, the deployment of a fully standard curriculum can only be described through a rational and explicit framework of requirements. The detailed process for creating and deploying those requirements is what is presented in these chapters.

Chapter One: Introduction: Securing Cyberspace Is Everybody's Business This chapter explains the general conditions under which the CSEC2017 was created. It outlines the problems with cybersecurity as we currently understand them. It also presents the background of the CSEC2017 and the role of the Learned Societies in creating it. The goal of this chapter is to give the reader an understanding of the overall strategic concerns associated with cybersecurity practice as well as provide the justification and advantages of a generally accepted common body of knowledge.

Readers will see how the lack of a unified understanding impacts everybody's security. The readers will also understand the reasons why the Learned Societies are so crucial in fostering common agreement in academia. They will see the justification for the actions taken by these societies to ensure a single comprehensive presentation of the elements of the field. Finally, this chapter will outline the eight knowledge elements of the CSEC2017 model.

Chapter Two: The Cybersecurity Body of Knowledge Development and coordination of a curriculum requires a common and coherent point of reference. The overall basis that is outlined in this chapter will give educators

a practical understanding of the structure and content of a typical standard curriculum. The goal of this chapter is to provide readers with the ability to create practice-oriented courses on the CSEC2017 model. The reader will learn why a formal, comprehensive body of knowledge, which is aimed at ensuring capable understanding of the elements of the field, is critical to curricular success.

The aim of this chapter is to help the reader understand the role and application of bodies of knowledge in the development of cybersecurity curricula. It will also help the reader understand how bodies of knowledge are used to shape new fields of practice. This chapter will go into depth on the rationale and potential applications of a commonly accepted body of knowledge for cybersecurity. It will also present the knowledge areas of the CSEC2017 in detail. Finally, the constituent elements of each of the knowledge areas will be presented and discussed. Subsequent chapters will discuss how each of these areas fit. The aim here is to provide a rational overview. By the end of this chapter, the reader will understand the typical process for curricular planning, including the necessary learning objectives.

Chapter Three: Knowledge Area One: Data Security The Data Security knowledge area is the perfect area to lead off the body of knowledge. Data Security defines what must be known in order to ensure the security of data assets either at rest, during processing, or in transit (CSEC, 2017). This is a well-accepted and commonly understood part of the current discipline of cybersecurity, and there is no disagreement about its importance in the overall protection of electronic assets. The knowledge elements associated with this protection process include the usual set of commonly acknowledged areas such as basic cryptography concepts, digital forensics concepts, and methods for secure communications, including data integrity and authentication and information storage security (CSEC, 2017).

Thus, this chapter provides an in-depth discussion of Data Security. It will help the reader understand how cryptography is an enabler for assurance. It will show how data integrity and authentication techniques are used to mitigate password attacks. It will discuss the role of access control in preserving Data Security and integrity. It will discuss the communication protocols that offer the best levels of Data Security. It will also consider the importance of cryptanalysis in securing data.

Chapter Four: Knowledge Area Two: Software Security This is another area nobody will find surprising. Software assurance goes back to the very origins of the field. So, it predates any concerns about security. In the 1990s, the methods and techniques in this area focused on creating defect-free code, and the general area of practice was called “software quality assurance” or SQA. Since most of the knowledge, skills, and abilities (KSAs) associated with SQA

transfer to the identification of exploitable flaws, the knowledge elements for this area are well defined and commonly accepted as accurate among both academics and business people.

The focus of the CSEC2017 Software Security knowledge units is on common assurance of the security properties of the information and systems that the software protects (CSEC, 2017). Thus, the CSEC2017 recommendations center on such accepted areas of practice as security requirements, design concepts and practice, software implementation and deployment issues, static and dynamic testing, configuration management, and ethics, especially in development, testing, and vulnerability disclosure (CSEC, 2017).

Chapter Five: Knowledge Area Three: Component Security The Component Security knowledge area is perhaps the most novel of the cybersecurity areas in that it is not an element of most of the predecessor bodies of knowledge for cybersecurity. However, it is not surprising to see it here given the inclusion of computer engineering in the issues of cybersecurity assurance. Component Security's body of knowledge focuses on the design, procurement, testing, analysis, and maintenance of the tangible components that are integrated into larger systems (CSEC, 2017).

Thus, the elements of this area include such well-accepted hardware aspects as identification and elimination of vulnerabilities present in system components, component life cycle maintenance and configuration management, secure hardware component design principles, security testing, and reverse engineering. Finally, there is although a healthy dose of supply chain management security knowledge elements due to the industry's commitment to commercial off-the-shelf integration of components.

Chapter Six: Knowledge Area Four: Connection Security This area is what is colloquially known as, "network security." The security of networks is another quality that is both commonly accepted as well as an essential aspect of good cybersecurity practice. So, it is not surprising to find it featured as an element of the body of knowledge.

Networks and networking have been a fundamental element of the information technology universe since the late 1960s, with ARPANET and other primordial computer communication systems. And networking had reached a high degree of sophistication prior to the advent of the Internet. But the security of networks became a primary concern with the introduction of that groundbreaking technological advancement. The knowledge in this area focuses on the security of the connections between components including both physical and logical connections (CSEC, 2017).

Thus, the CSEC2017 guidelines entail assurance practices for networked systems, networking architecture, and standard secure transmission models, physical component interconnections and interfaces, software component interfaces, and of

course, the common types of connection and transmission attacks.

Chapter Seven: Knowledge Area Five: System Security This knowledge area begins the move off of the technology platform and into the area of standard organizational processes. Hence, the System Security knowledge area focuses primarily on those common organizational practices that ensure the security requirements of systems, which are composed of interconnected components and connections, and the networking software that supports those interconnections (CSEC, 2017).

Accordingly, the knowledge elements in this area embody guidelines that spell out the necessity for a holistic approach to systems, the importance of security policy, as well as organized identification and authentication management processes; this area also contains recommendations for system access control and operational system monitoring processes, as well as the standard recovery, system testing, and system documentation best practices.

Chapter Eight: Knowledge Area Six: Human Security This is a brand-new and very novel element of the body of knowledge. It represents the first serious attempt to provide recommendations with respect to the human attack surface. As we have said, this is terra incognita for the traditional study of cybersecurity, so, although it might not be as mature as areas one through four, it represents a pioneering step in the effort to compile a complete and correct body of knowledge for the field.

The first four knowledge areas comprise what might be considered to be the "usual suspects" in the cybersecurity profession. They are essentially hard, technology focused, elements that encompass generally well-known and commonly accepted axioms regarding the practice of data, software, component, and system assurance. The Human Security area attempts to make benchmark recommendations about the assurance of human behavior and the study of human behavior as it relates to the maintenance of a state of cybersecurity.

Needless to say, this is a new area and one which will probably be susceptible to refinement over a period of time. However, the loss statistics make it clear that the focus on protecting individuals' data and privacy in the context of their role as employees and in their personal lives is an important area of teaching and research (CSEC, 2017). The recommended knowledge elements in the Human Security knowledge area include such areas as identity management, social engineering prevention, assurance of workforce and individual awareness and understanding, assurance of broad-scale social behavioral privacy and security, and the elements of personal data privacy and security protection.

Chapter Nine: Knowledge Area Seven: Organizational Security Organizational security is historically the most well-known and commonly discussed aspect of

all of the nontechnical areas. The general content and focus of this area is embodied in the recommendations of the National Institute of Standards and Technology's workforce framework (NIST 800-181) as Knowledge Area Seven, "Oversee and Govern" (Newhouse, 2017).

The Organizational Security area encompasses all of the relevant processes and behaviors for the rational oversight and control of the overall cybersecurity function. This is understandably a very large element of the CSEC2017 model, since those controls embody all of the traditional countermeasures that are associated with the general protection of the organization as a whole. This includes the deployment and oversight of controls to ensure proper monitoring and response to intrusions on the technological attack surface, as well as the entire set of standard behaviors associated with the human attack surface.

The purpose of the knowledge that is embodied in the Organizational Security area is to assure the organization against all relevant cybersecurity threats, as well as manage the inherent risks that are associated with the successful accomplishment of the organization's mission (CSEC, 2017). Consequently, the elements in this area include a detailed set of recommendations for the risk management process, the setting of governance and policy strategies, long- and short-term planning, as well as legal, regulatory, and ethical compliance.

Chapter Ten: Knowledge Area Eight: Societal Security The Societal Security knowledge area is revolutionary, and it reflects the growing awareness of the impact of virtual space on the average person's life. The knowledge items in this category are mostly large societal factors that might, for better or for worse, broadly impact every citizen in our society.

The knowledge elements are essentially still in need of refinement. But their inclusion opens the door to their integration into the overall understanding of how virtual space needs to be channeled into institutional actions that area beneficial to the world community as a whole. This includes thought models for approaching the problems of cybercrime, the legal and ethical dictates associated with good citizenship, as well as social policy, personal privacy, and how that relates to the formal mechanisms of conventional cyberspace (CSEC, 2017).

The specific recommendations promulgated in this area center on the general behaviors to prevent, or alleviate cybercrime, make and enforce laws in cyberspace, ensure ethical thinking when it comes to functioning in cyberspace, as well as the elements of what constitutes proper cyber policies and privacy regulation.

Reader Expectations

This book presents a set of well-defined and commonly accepted knowledge requirements for building recommended curricula in cybersecurity. Therefore, there are no expectations about specialized technical knowledge per se. All readers will learn how to design and develop a commonly sanctioned curriculum in cybersecurity using the holistic recommendations of the CSEC2017 model. After reading this book,

the reader will know how to build and maintain a complete, applied curriculum that conforms with the principles of best practice, as well as evolve the curriculum to continue to meet the learning requirements for the field as they evolve. At the end of this book, the reader will be able to:

- Create, sustain, and evolve a holistic cybersecurity curriculum.
- Define and evaluate instructional processes and supporting material.
- Ensure full and complete coverage of all of the essential elements of the discipline of cybersecurity.

References

CSEC, Joint Task Force (JTF) on Cybersecurity Education, "Cybersecurity Curricula 2017, Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity, a Report in the Computing Curricula Series," ACM/IEEE-CS/AIS SIGSEC/IFIP WG 11.8, Version 1.0, 31 December 2017.

Newhouse, William, Stephanie Keith, Benjamin Scribner, Greg Witte, "NIST Special Publication 800-181, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework," NIST.SP.800-181, August 2017.

1

Securing Cyberspace Is Everybody's Business

In this chapter, you will learn the following:

- Why a standard definition of the practice of cybersecurity is important
- How exploitable gaps occur in a real-world cyberdefense
- The importance of teaching cybersecurity as comprehensive process
- The role of professional societies in shaping the discipline of cybersecurity
- The general structure and intent of the CSEC2017 Project
- The practical applications of the CSEC2017 Project.

Introduction: The Current Situation Is Out of Control

It is a well-documented phenomenon that there is a global problem securing cyberspace (Accenture, 2019; Rivero, 2018; Hatchimonji, 2013; Symantec, 2014; Trend-Micro, 2015; PRC, 2017; NIAC, 2018). However, the price of that failure might not be so clear. To use a couple of global concerns to illustrate the problem, first, let's look at the skyrocketing cost of cybercrime. In 2015, cybercrime cost the world $500 billion. By 2018, that expense had escalated sixfold to $3 trillion (Microsoft, 2018). And, by 2021, the price is expected to double again to $6 trillion (Microsoft, 2018). Needless to say, an annual loss that exceeds the combined gross domestic product of Great Britain, Germany, and France combined is going to impact every business in every industrialized country in the world (Figure 1.1).

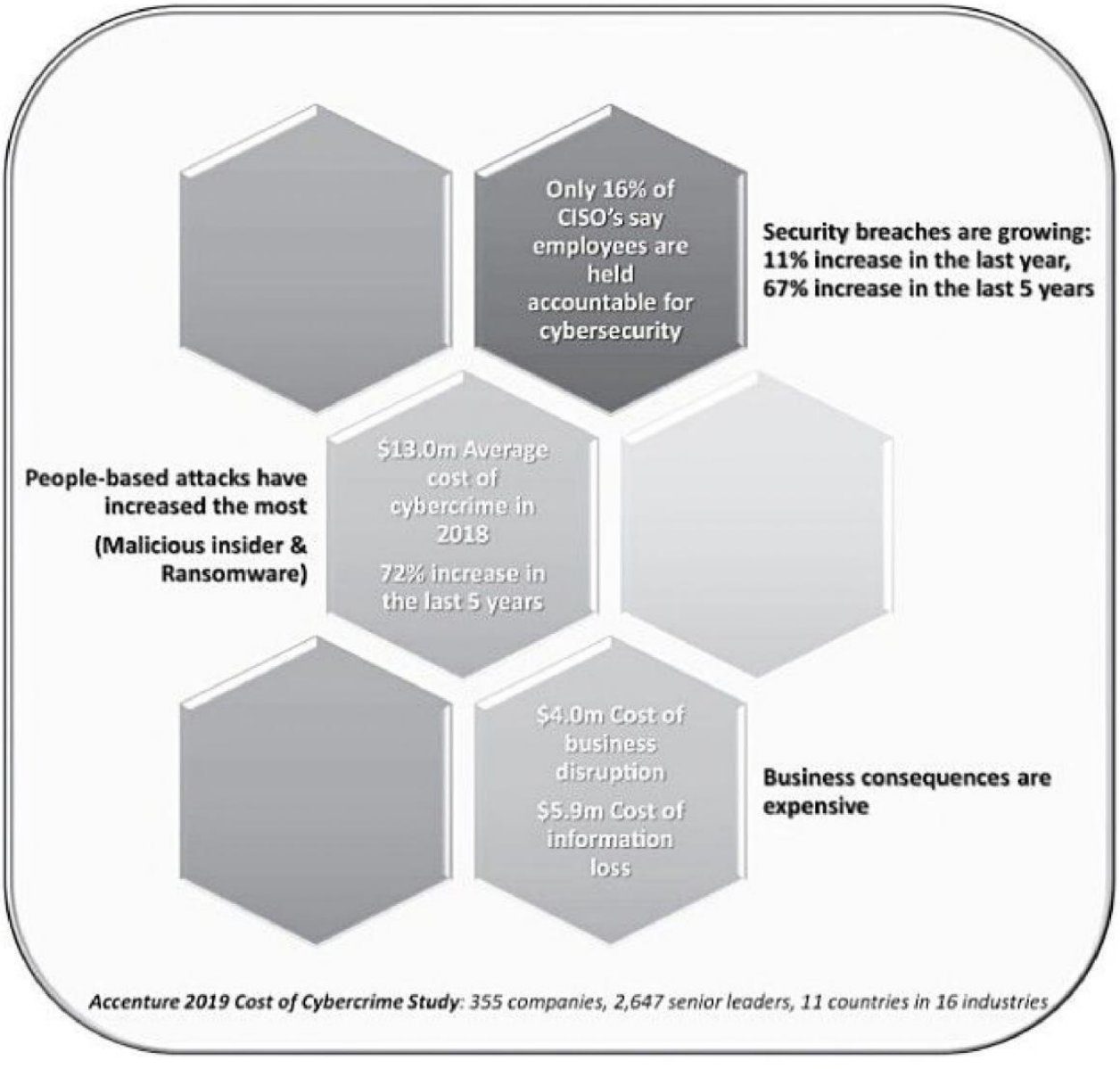

Figure 1.1 Global problem of securing cyberspace.

Additionally, there are advanced persistent threats in cyberspace that target our critical infrastructure, and since the infrastructure underwrites our entire way of life, the prospect of harm to it is a threat to our national survival (NIAC, 2018; Cummins & Pollet, 2009). A potential attack on any major element of our infrastructure is so strategically significant that it has been dubbed as a "Digital Pearl Harbor." The basis for the concern is that much of the infrastructure was designed before the need to protect it was even an issue (NIAC, 2018). So, the automated functions that perform the infrastructure's everyday tasks have no innate resistance to a cyberattack. Still, those components are at risk only if they are remotely accessible (Figure 1.2).

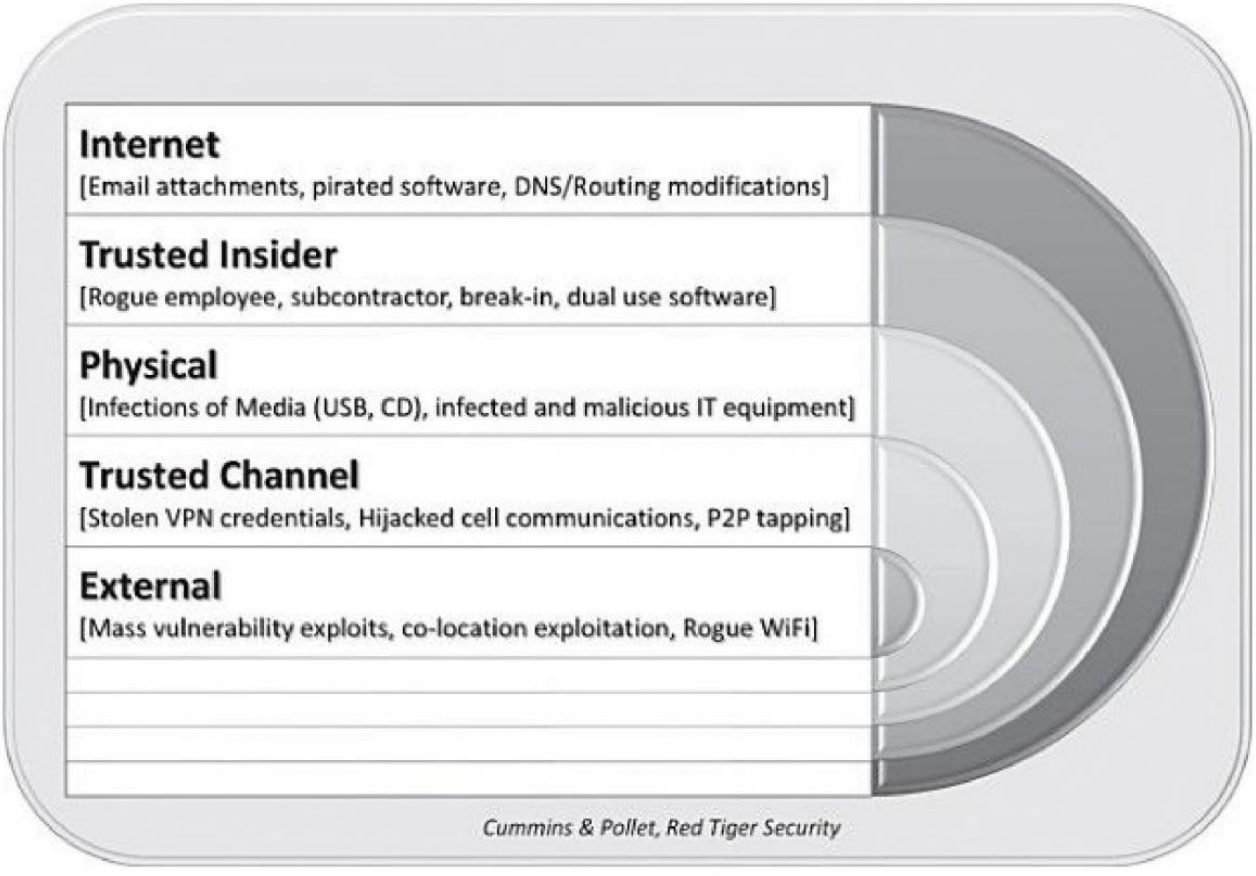

Figure 1.2 Advanced persistent threat vectors.

There is an increasing propensity to hook infrastructure components to the Internet for ease of maintenance and operation, which makes the whole architecture almost impossible to defend. This is the reason why the issue of cybersecurity is a serious part of any discussion about our national interest.

What has been our society's response? Unfortunately, the response has been to dither (Brasso, 2016). Specifically, none of the sectors in the United States' national infrastructure domain have developed an effective strategy or a coherent scheme to protect itself from a concerted cyberattack (NIAC, 2018). And even worse, there is no consistent agreement about what would constitute such an attack (Brasso, 2016). Yet a successful attack on any major element of the national infrastructure could literally end society as we know it (NIAC, 2018).

Consequently, infrastructure cybersecurity now epitomizes the sort of existential threat that nuclear war used to pose. Will such a thing ever happen? In the words of Mike Rogers, the former head of the National Security Agency, "It's not a matter of if, but when!" (NIAC, 2018; Lois, 2015). Thus, it is critically important that we address the significant issues in cyberspace.

The Challenge: How Do You Protect Something that Doesn't Actually Exist?

You would think that every organization's top priority would be the creation of a complete and comprehensive virtual asset protection scheme. However, cybersecurity

is treated a lot like the weather; everybody talks about it, but little is done to seriously address it. For example, only 38% of the organizations that were surveyed by Information Systems Audit and Control Association (ISACA) in its "2015 Global Cybersecurity Status Report" felt that they were taking substantive steps to address the problem of cyberthreat (Laberis, 2016).

The Internet has the same potential impact on society as the invention of moveable type. The difference between these two revolutions is that our culture took three centuries to accommodate to the profound impacts of mass printed information. Whereas, we've had a mere twenty years to adjust to the even more momentous impact of immediate access to every virtual thing in the world. Accordingly, it is not surprising that society's mechanisms have had a hard time keeping up (Figure 1.3).

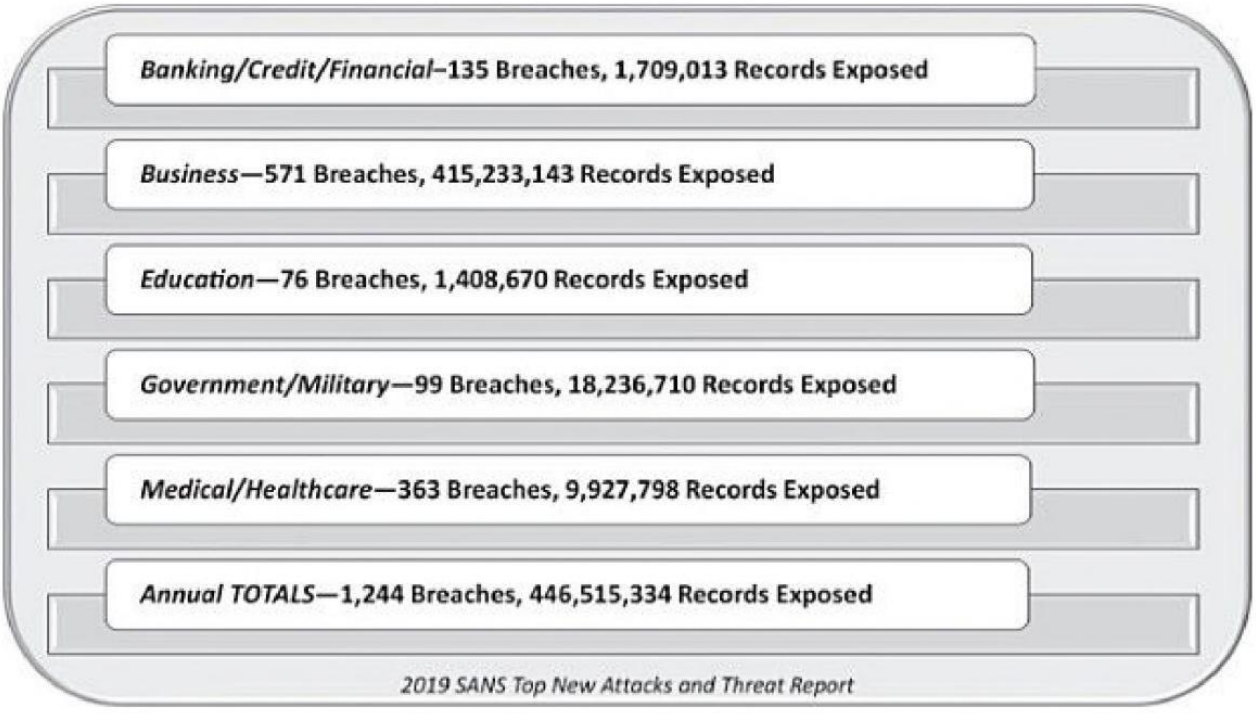

Figure 1.3 2018 security breaches.

A protection scheme that is unable to guarantee the reasonable confidentiality, integrity, and availability of its protection objects has not achieved its basic purpose. It should be noted here that there is no exception to this rule. A loss of virtual value is a loss, no matter how the exploit was actually carried out. So, it's a moot point whether it was an insider exploit or an electronic attack. It was still a loss.

The single characteristic by which a cybersecurity effort ought to be judged is its ability to dependably and effectually prevent any type of loss or harm to an organization's virtual assets. In this respect, it is axiomatic that the cybersecurity function is obliged to close off every potential avenue of attack for all of the virtual assets that it is held accountable for. And ten years of data loss makes it crystal clear that we are getting worse at the task, not better (Figure 1.4).

Top 10 Data Breaches of All Time

Company	Accounts Hacked	Date of Hack
Yahoo	3 billion	Aug. 2013
Marriott	500 million	2014-2018
Yahoo	500 million	Late 2014
Adult FriendFinder	412 million	Oct. 2016
MySpace	360 million	May 2016
Under Armor	150 million	Feb. 2018
Equifax	145.5 million	July 2017
EBay	145 million	May 2014
Target	110 million	Nov. 2013
Heartland Payment Systems	100+ million	May 2008

Figure 1.4 Top ten security breaches of all time.

We Must Re-evaluate Our Assumptions

In 1929, Lieutenant Colonel J.L. Schley wrote in the *Military Engineer*, "It has been said critically that there is a tendency in many armies to spend the peace time studying how to fight the last war." And this has never been truer with the fight to protect cyberspace. On the surface, the justification for our current approach seems simple enough. The virtual world is enabled by computers, which have an explicit set of rules associated with them. These rules are dictated by the unyielding architecture of the machine. Therefore, it seems obvious that we should base our cybersecurity protection paradigms around the well-established scientific principles of computer engineering and networking architecture, which has been the reasoning since the beginning of the field. However, perhaps we have misunderstood the meaning of the term "cybersecurity."

Cybersecurity is a combination of the words cyber, meaning *computer* and *security*. We understand the reason for the cyber part. Virtual information is kept and transmitted electronically by computers so, it seems like common sense to hand the responsibility for cybersecurity to the technical part of the organization. The problem is that *security* is actually its own independent concept and it carries a different set of requirements. Security implies the act of safeguarding something. Cybersecurity, as

the term is presently interpreted, does protect some things. For instance, it is well documented that the effective percentage of successful electronic exploits has decreased over the past decade. Even so, it is one thing to protect a virtual asset from unauthorized electronic access, while it is another thing entirely to ensure that the same asset cannot be lost or harmed due to any type of credible exploit or attack.

In this respect, the *security* part of *cybersecurity* expands the protection mission to encompass the responsibility to safeguard every virtual object of value. Thus, cybersecurity's role goes from simply regulating the coming and going of data through a highly restricted point of electronic access, like a firewall, to assuring that the virtual asset cannot be harmed by any foreseeable means. The latter requirement is a much more rigorous test. But it is still an inescapable fact that, a loss of value is a loss no matter what the cause is (Figure 1.5).

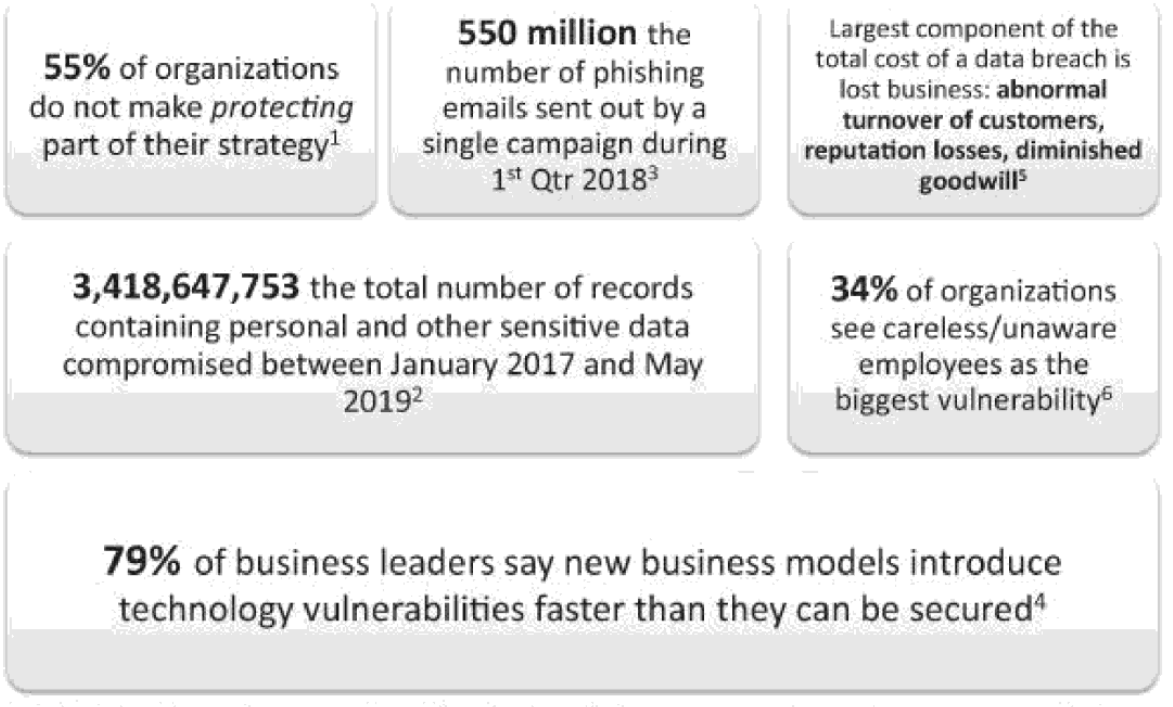

Figure 1.5 Organizational responses to cybersecurity.

There are two highly credible types of attacks that are unavoidably part of the overall attack surface: human and physical exploits. The willingness of an organization to ignore these plausible lines of attack will preprogram failure into the protection mission. Current research shows that electronic exploits constitute less than one-third of the threat. The rest of the protection problem involves such real-world factors as insider threats and social engineering or even natural complications like fire or flood. So, the question remains, who should be responsible for deploying and coordinating a defense against those types of exploits?

In many organizations, human or physical types of threats are often not included in traditional cyberdefense planning. Most active cyberdefense solutions do not even

consider the need to embody tightly integrated, well-defined, and uniformly applied behavioral controls as a fundamental part of the overall cybersecurity process (Laberis, 2016). As a result, well-executed attacks against the nonelectronic attack surface are almost certain to succeed. The question is, what is the reason for such a clear disconnect in our planning?

The Adversary Changes Things

The goal of the adversary is to break into the system, not use it. And those adversaries are not constrained by conventional rules of engagement. Besides the traditional task of ensuring that the system operates as intended, system developers and administrators are now expected to ensure that its day-to-day functioning is fully safeguarded from any foreseeable kind of malicious exploitation. In the case of a determined adversary, the scope of the protection perimeter is now opened up to any means necessary to achieve the ends of a wide range of hacker types. If the adversary's aim is to subvert or acquire a virtual asset, then the easiest way to accomplish this would be through the path of least resistance (PRC). As far back as the 1970s, Saltzer and Schroeder codified this as the *Work Factor* principle (Saltzer and Schroeder, 1974). In essence, the adversary will adopt the approach that is the easiest to execute and the most likely to succeed. Sun Tzu characterized this thinking best when he wrote, "Attack weakness not strength." Or in practical terms, the form of the hack will be dictated by the shape of the soft spots in the cyberdefense.

If the organization has constructed a strong electronic defense, a smart adversary will launch anything BUT an electronic attack and the data supports this. In 2006, the predominant percentage of loss was from exploits that could be classified as "electronic" (PRC, 2017). Fast forward and the preponderance of the losses are due to exploits that are classified as "behavioral" (PRC, 2017). This change in tactics illustrates how the adversary has simply shifted their line of attack to accommodate our improved capability in the electronic realm. And since the nontechnical attack surface is so much wider, it is also, most probably, the reason why our loss statistics continue to grow at exponential rates.

From a terminology standpoint, the exploits we have been talking about are nontechnical hacks. Both human-centered and physical types of attacks fall into that category and, as the term implies, nontechnical hacks that do not target the technology directly. Rather than electronic types of approaches, nontechnical hacks increasingly target existing behavioral or physical weaknesses in the organization. Thus, in real-world terms, nontechnical hacks are aimed at the human attack surface. The term *human attack surface* simply denotes every possible way in which intentional behavior that is executed in the physical space could compromise an asset or its confidentiality. Microsoft estimates that by 2020, the human attack surface will encompass 4–6 billion people (Microsoft, 2018).

Because human behavior is distinctive, creative, and unpredictable, there are an infinite number of ways that a nontechnical hack can be executed. The most popular approaches include such familiar exploits as insider and social engineering attacks. But nontechnical impacts can also be the result of humble everyday operational errors

like procedural malfunctions and even simple worker negligence (Whatis, 2018).

It is hard to estimate the percent of actual harm that nontechnical hacks represent. Damaging exploits, such as industrial espionage or theft of proprietary trade secrets, are rarely reported, and simple human negligence or inadvertent error tends to get missed or covered up. Therefore, it is impossible to accurately describe the impact of such a set of occurrences. Nevertheless, it is believed that the overall extent of the problem is most certainly far greater than what is currently estimated (Laberis, 2016).

There are two logical reasons why nontechnical hacks go unreported or, for that matter, unnoticed. Both of them illustrate the challenge organizations face when it comes to building a complete and effective cyberdefense. First, companies, and particularly top-level decision makers, simply don't associate human behavior with virtual losses and so the threats that malicious insiders and bumbling employees represent tend to fly under their radar (Laberis, 2016). Nevertheless, nontechnical hacks are now the dominant PRC (2017). And since the adversary is becoming more and more reliant on their use, we will have to learn how to close off all the alternative paths. The ability to identify, classify, and counter nontechnical exploits will have to be amalgamated into every organization's overall understanding and approach to cybersecurity going forward.

Second, human behavior is impossible to accurately predict or effectually monitor. More importantly, an insider is part of the organization; therefore, they are trusted to some extent. Accordingly, it is almost impossible to spot a capable insider who is planning to undertake an attack, and because humans are creative, their harmful actions are almost impossible to assure by automated means (Laberis, 2016). Yet, most of our present-day cyberdefenses are still exclusively oriented toward countering electronic types of attack, which is also reflected in the loss statistics.

At present, 71% of annual losses are due to failures in the physical and human attack domains, while electronic breaches account for roughly 29% (PRC, 2017). Specifically, the leading cause of record loss (36%) over the past decade is attributable to physical exploits (PRC, 2017). A physical exploit is any hands-on theft, harm, or loss. A stolen laptop containing sensitive information is one example. Human behavior is the second leading cause of record loss (35%). Human behavior exploits include such categories as insider theft, social engineering, or human error (PRC, 2017). While the lowest percentage of losses (29%) fall into the area of the classic technology-based attacks, unfortunately, these are often the only kind of attacks factored into an organization's cybersecurity planning.

The Three-Legged Stool

Cyberdefense rests on a three-legged stool: electronic, human, and physical. The practical starting point for good cyberdefense is to begin to assimilate the three important areas into the overall strategic planning function; however, one issue is that the three component domains have traditionally operated independent of each other. So, the question is, how do we start the process? We start by knocking down the stovepipes. Stovepipes, where teams work independently of each other and do not share information, are the reason that credible threats like insider attacks or social

engineering need to be called out and addressed in the formal protection planning process (Figure 1.6).

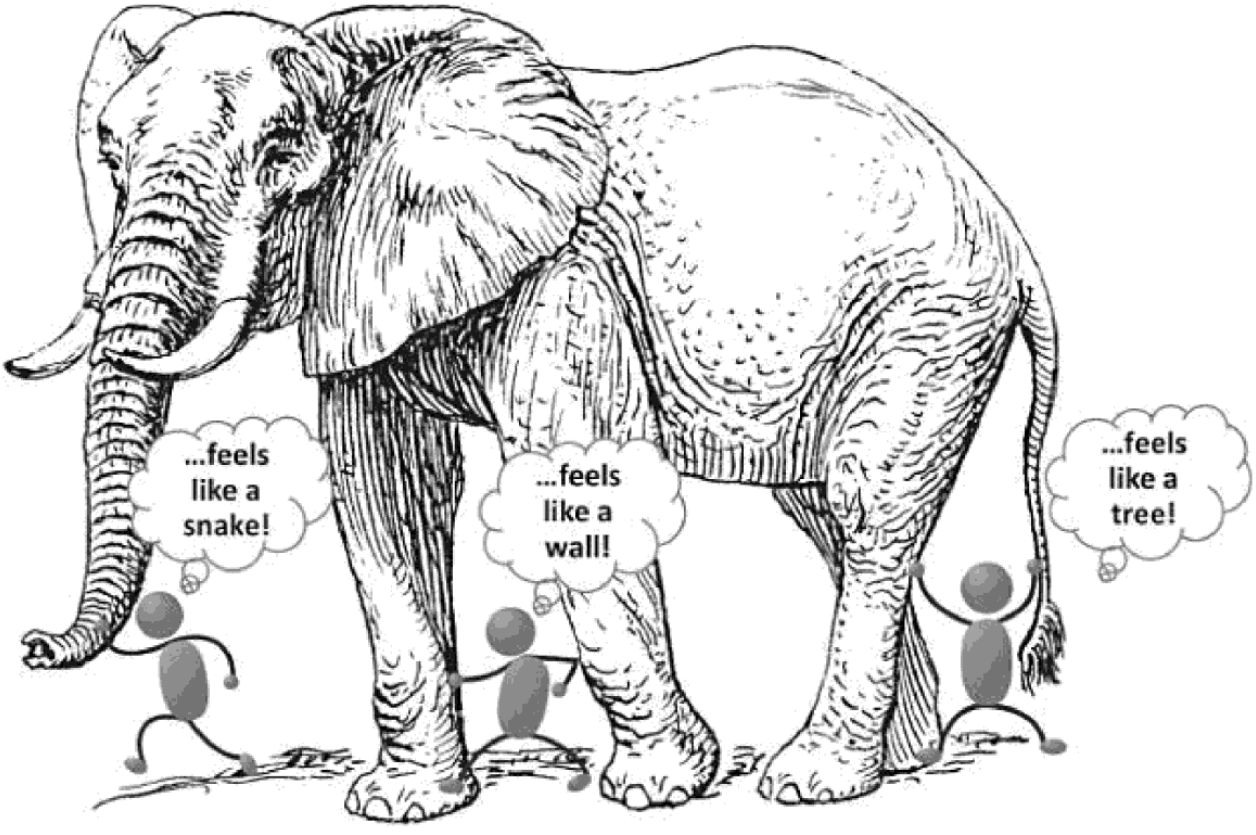

Figure 1.6 Blind men and the elephant.

The people who should be involved in constructing the cybersecurity defense may not be aware of the aspects of the problem that they do not touch because of the blind men and the elephant syndrome. In that old fable, six blind men are asked to describe an elephant based on what they are touching. To one, it's a snake, to another it's a wall, and to another it's a tree, etc. But in the end, "Though each was partly in the right, all were entirely wrong."

So, the need to counter threats that arise in other areas is overlooked. Understandably, the job of network security is to secure the network, not necessarily the software applications, just as human resource personnel do not configure firewall rules or restrict access control to servers as part of their mandate. The present stovepiped state of the practice is leveraged by at least three mutually limited views of the world, which puts the cybersecurity function into an unavoidably dysfunctional state. Although there are established elements of the field that can capably protect the part of the elephant that they touch, none of the conventional elements are an entirely effective solution in and of itself. And if every practical aspect of the solution is not fully integrated into the response, then the PRC gaps are bound to manifest.

Learning to Play Better with Others

Exploitable gaps are created when the important actors in the cyberdefense process

do not collaborate. As we have seen, most of the necessary set of actors are probably unaware of the actual requirement to cooperate. For instance, the failure to lock and monitor the computer room or to thoroughly vet the system manager will always invalidate any elegant security solution. This is because direct access to the machine trumps every other form of countermeasure.

These situations are sources of the types of *exploitable gaps*; however, the design of substantive steps to limit every form of direct physical access to the server, such as locks and employee monitoring and supervision, requires participation of the relevant players from the human resources and physical security areas. Often, these experts are not involved in either the planning or the day-to-day operations of the cybersecurity function.

Every factor has to be considered in order for a cyberdefense to be gap-free. But, because the planning for cybersecurity is often seen as a strictly technological exercise, the organization is not able to deploy the full set of controls necessary to completely and adequately protect its assets from every conceivable source of harm. Accordingly, the challenge is clear. The profession must find ways to ensure that the real-world practice of cybersecurity incorporates a complete, accurate, and highly effective set of well-defined and commonly accepted controls – ones that are capable of closing off every feasible type of adversarial action.

Creating a Holistic Solution

The term *holistic* was adopted to describe a state of comprehensive cybersecurity. Holistic simply means that every type of threat has been identified and countered by a formal control mechanism. In practical terms, holistic solutions describe organizational situations in which all likely threats have been effectively countered by an actual and fully integrated set of electronic, physical, and human-centered controls and are enabled by a systematic planning process. Therefore, good cybersecurity practice involves strategic architecture and design. The architectural process must consider all reasonable avenues of exploitation and all of the necessary controls and countermeasures are implemented and enforced. The aim of the countermeasures is to ensure a complete and effective cyberdefense. This isn't just a matter of putting together a list of controls. There has to be a specific organizational mechanism in place to rationally integrate every one of these controls into a complete and effective cyberdefense system.

The Importance of Knowing What to Do

We will only be able to implement a holistic solution when we are able to bring all of the essential players together. Since the consolidation of protection responsibilities is likely to incorporate a range of skills and interests, there must be a universal agreement about the elements that constitute correct and effective practice. To be fully effective, the definition must amalgamate all of the essential concepts of cyberdefense into a single unifying practice model; one that has real-world currency.

Best practice is not something that is empirically derived. The term "best practice"

simply designates the things that we know as a result of universal lessons learned over time. Best practice is classically embodied in "Bodies of Knowledge" (BOK) which is founded on expert opinions about the best way of doing something. The purpose of the rest of this book is to explain how a common body of knowledge is derived and conveyed, as well as how it can be a difference maker for educators in designing proper curricula and courses.

Enabling Common Understanding

Every profession is built around a common understanding of the appropriate and effective practices of the field. A formal statement of the critical underlying knowledge requirements is the necessary point for building an academic discipline and should serve as the basis for understanding what needs to be studied. The basic knowledge requirements tell the educator and student what they need to know and do, and it helps them understand how all of the elements of their field fit together as they relate to a real-world understanding of the basic responsibilities of the cybersecurity professional.

Up to this point, there has never been a legitimate commonly accepted definition of the critical elements that would constitute the knowledge required to do cybersecurity work. This key missing definition was what motivated the production of the National Institute for Standards and Technology workforce framework (NIST 800-181). NIST prepared the model as a definition of the standard roles in the cybersecurity workforce and is very useful in that respect. It demarcates the limits and job categories of every practical area of work in the profession. It also describes the common knowledge, skill, and ability (KSA) requirements for each area. However, while NIST 800-181 is an excellent first step, its application is still limited to the federal government space.

The government has provided outstanding leadership in the definition of the field. But it has a different role and function than classic institutions of education. As a result, NIST 800-181 still does not represent the essential commonly accepted body of knowledge that educators need to build curricula and courses. Therefore, an officially sanctioned body of knowledge was still the missing link in the formal education process.

Education Is the Key

Education has been the societal entity responsible for embedding new ideas in a culture. Academic scholars conduct research to add to the body of knowledge; however, the practitioner societies (associations) have traditionally developed and documented the essential concepts of the academic fields and their experiences working in organizations. Skilled and experienced practitioners are the entities who are typically most current on the issues that organizations face and the logical people to provide a body of knowledge for cybersecurity. The culmination of the work of the leading cyber associations is the CSEC2017 model, which is discussed in the rest of this text. CSEC2017 should be considered to comprise the single authoritative statement of

the knowledge elements that unify the various elements of the field of cybersecurity into a single common vision, and in that respect, CSEC2017 is the first step in defining a stand-alone field of study for cybersecurity.

The Body of Knowledge and Educational Strategy

Along with the coordinated management of the classroom delivery of content, any emerging discipline requires a formally planned and implemented, broad-scale academic strategy. A clear-cut educational approach is the underlying condition that is necessary to impart knowledge in every organized discipline of study from dentistry to mechanic's school. Yet, up to this point, the elements of the field of cybersecurity have not been embodied in any form of all-inclusive strategic direction; particularly where the human attack surface is concerned.

A standard educational delivery approach is made difficult without a communal understanding and acceptance of a credible body of knowledge. All of the participants in the teaching process have to be on the same page in order for the message to be sufficiently well coordinated. So logically, the first requirement for formulating a cogent educational approach is common acknowledgment of what appropriate learning content is for a given study. The requisite knowledge has to be actively identified, catalogued, and disseminated. For example, computer science didn't just show up in college catalogues in one day. It evolved over time as an amalgam of fundamental ideas from the fields of mathematics, electrical engineering, and even philosophy. Subsequently, the official contents of that body of knowledge had to be sanctioned as correct by the relevant practitioners in order to make the study of computer science into a formal educational discipline. Then after that recognition, the body of knowledge had to be formally promulgated to all pertinent educational providers in a systematized fashion.

In academe, the formal mechanism for promulgating BOK are the learned societies that are generally acknowledged as being the legitimate overseers and sanctioners of that particular academic discipline. Every legitimate body of knowledge has to be accepted as accurate by the profession it characterizes and is typically obtained from expert advice about lessons learned in the real world. Professional societies exist and serve as the developers and sanctioners of the fundamental ideas in their respective fields. Thus, it is the professional societies who are responsible for the promulgation and accreditation of a recognized body of knowledge and professional practice. Examples of professional bodies include well-known groups such as:

- The American Medical Association (AMA) for Doctors
- The American Dental Association (ADA) for Dentists
- The American Bar Association (ABA) for Lawyers
- The National Society of Professional Engineers (NSPE) for Engineers

In the case of computer science, interest groups, which are termed "learned societies," have promulgated curricular guidelines for their areas of interest, and each of these societies now sponsors a particular academic discipline. The Association for

Computing Machinery, or ACM, sponsors computer science; the Institute of Electrical and Electronic Engineers (IEEE) sponsors software engineering; the Association for Information Systems (AIS) sponsors business information systems; and the International Federation for Information Processing (IFIP) expands the sanctioning of best practice for each of these areas into the international arena (Figure 1.7).

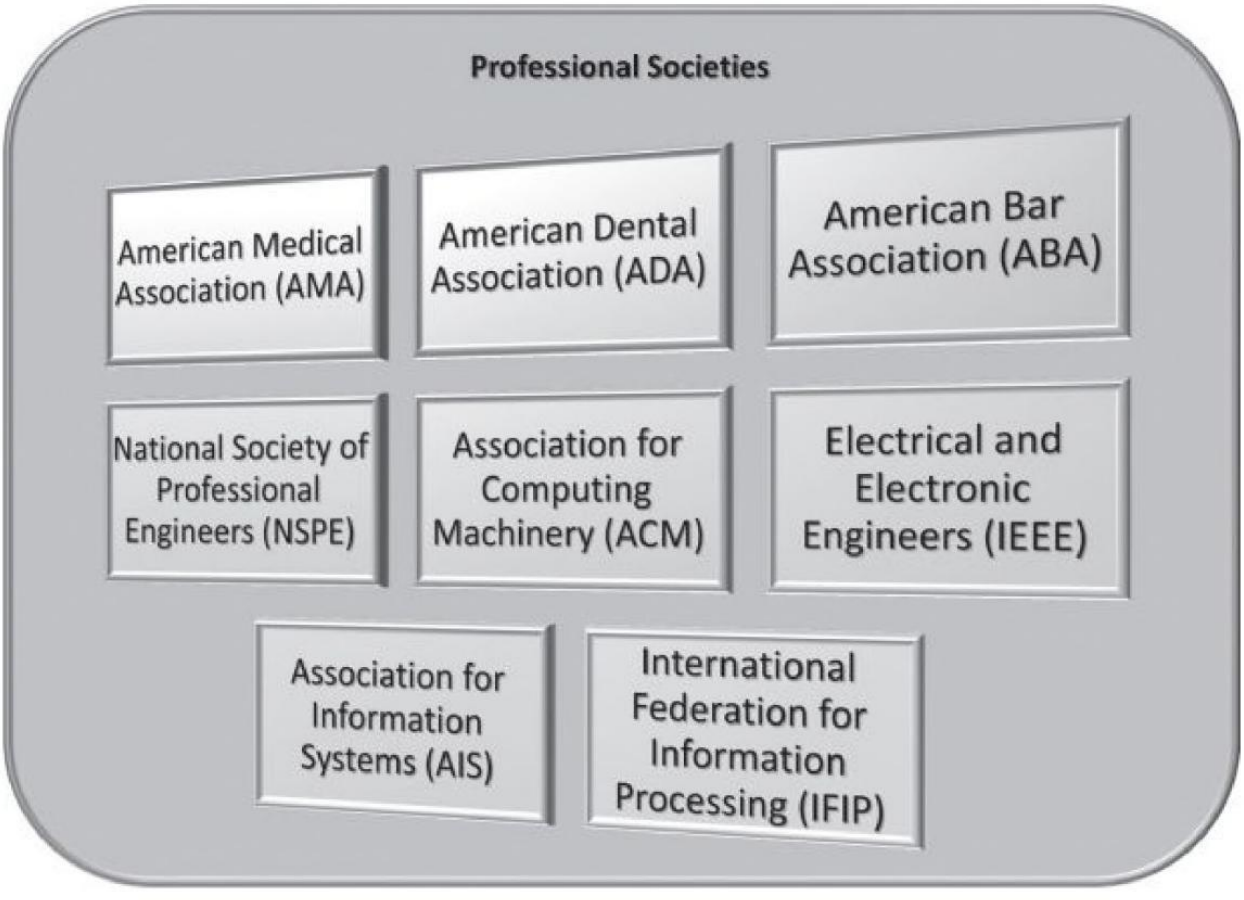

Figure 1.7 Professional associations.

Because computing comprises more than just the science of the computer, over time, other professional and academic interest groups have come together to address the issues in their particular areas. These groups are also involved in establishing guidelines for the BOK as they apply to their specific educational interests. At this present point in time, standardized recommendations for curricula are available for the disciplines of computer science (2013), computer engineering (2016), information systems (2010), information technology (2017), and software engineering (2014) (ACM, 2018).

Cybersecurity as an Academic Study

The four commonly recognized "societies" that sanction the aspects of the field of computing from oldest to newest, are the ACM, the IEEE, the AIS, and the IFIP. Their role is to define the acceptable knowledge for their respective areas of practice as well as maintain standards of accuracy.

The Association for Computing Machinery (ACM)

ACM was founded in 1947 by the American computer scientist Edmund Berkeley. Today, it is the world's largest scientific and educational computing society with a membership of over 100,000 (ISCTE, 2018). ACM is considered to be an umbrella organization for all of the academic and scholarly concerns in computer science. ACM officially coordinates scholarly activities related to that discipline as well as serves as the formal spokesperson for the academic groups under its care.

ACM's activities include holding regular conferences for the presentation and discussion of new research in computer science as well as the publication of academic journals in subspecialty areas. This includes convening the Task Force that produced the CSEC2017 report. As the interest group for the study of computer science, the ACM also published CS2013, "Curriculum Guidelines for Undergraduate Programs in Computer Science."

The International Society of Electrical and Electronic Engineers (IEEE)

As the name implies, IEEE sponsors activities related to the field of electrical and electronic engineering. IEEE actually has its origins in the 1880s, which far predates the computer. However, the interest groups that comprise today's IEEE were not formed into the present entity until 1963. Currently, IEEE has over 395,000 members in 160 countries, and through its global network of geographical units, publications, web services, and conferences, IEEE remains the world's largest technical professional association (IEEE, 2019).

The IEEE is responsible for the development of engineering standards for the computer and electronics industry. IEEE has traditionally been the entity focused on professional application of engineering techniques and tools to improve the software industry. Specifically, relevant to the study of cybersecurity, the IEEE fosters the application of conventional engineering principles and methods for the software industry. As a result, IEEE publishes both undergraduate and graduate curricula for the discipline of software engineering. The discipline was formally sanctioned in 1987 (Ford, 1994). The current IEEE curriculum recommendations for the field of software engineering are SE2014, "Curriculum Guidelines for Undergraduate Degree Programs in Software Engineering" and GSwE2009, "Curriculum Guidelines for Graduate Degree Programs in Software Engineering."

The Association for Information Systems (AIS)

AIS was founded in 1994. It is the professional association that develops and promulgates knowledge and practices related to the management information systems profession. The society itself is mainly an academic association and is comprised of teachers and scholars who foster best practice in the development, implementation, and practical assessment of information systems.

AIS involves participants from more than ninety countries (AISNET, 2018), which

represent three regions of the globe: the Americas, Europe and Africa, and Asia-Pacific (AISNET, 2018). The association publishes academic curricula for the study of business information systems, *IS2002, Curriculum Guidelines for Undergraduate Degree Programs in Information Systems*, and the IS2010, *Curriculum Update: Curriculum Guidelines for Undergraduate Degree Programs in Information Systems*. It also publishes *MSIS2006, Model Curriculum and Guidelines for Graduate Degree Programs in Information Systems* (ACM, 2018).

The International Federation for Information Processing (IFIP)

IFIP is a nongovernmental entity responsible for linking the various national information technology associations working in the field of information processing. It serves as the umbrella interest group for all of the national societies in the field of computing. IFIP Technical Committees and Working Groups contribute to, and often lead, progress in the state-of-the-art knowledge and practice in information technology/information processing fields.

IFIP was established in 1960 as an outcome of the first World Computer Congress held in Paris in 1959. It operates under the auspices of UNESCO (IFIP, 2018). IFIP represents IT Societies from over fifty-six countries, spanning five continents with a total membership of over half a million people (IFIP, 2018).

The Importance of Unified Recommendations about Areas of Vital Interest

Occasionally all the societies come together to develop a single unified set of recommendations in the case of a topic of vital mutual interest. The first document of that type was the, *Joint Curricular Recommendations for Computing Curricula* (ACM, CC2005). CC2005 was developed to define the disciplines that were considered to be justifiably a part of the general study of computing. It was an important topic in the late 1990s because the out-of-control proliferation of disciplines that were centered on computer study and were both confusing and dysfunctional in education in general. Hence, CC2005 was significant in that it drew the line around and clarified the academic studies that could be considered to be the components of overall computer education.

After CC2005 was published, it became increasingly evident that a sanctioned definition of the elements of the emerging discipline of cybersecurity was also required. Thus, the societies once more organized a Joint Task Force to formulate the first set of globally accepted curricular recommendations for cybersecurity education (CSEC, 2017). The guideline is entitled the, "Cybersecurity Curricula 2017, curricular volume," or CSEC2017. The aim of CSEC2017 is to be, "The leading resource for comprehensive cybersecurity curricular content for global academic institutions seeking to develop a broad range of cybersecurity offerings at the post-secondary level." (CSEC 2017 Mission Statement, p. 10).

The recommendations of the CSEC2017 body of knowledge provide educators and their students with an authoritative understanding of the complete set of knowledge

16. The global impact of cybersecurity on a nation's culture
17. The global impact of cybersecurity on a nation's economies
18. The global impact of cybersecurity on a nation's social issues
19. The global impact of cybersecurity on a nation's policies
20. The global impact of cybersecurity on a nation's laws
21. The fundamental concept of privacy
22. The societal definition of what constitutes personally private information
23. The trade-offs between individual privacy and security
24. The trade-off between the rights to privacy by the individual versus the needs of society.
25. The common practices and technologies utilized to safeguard personal privacy
26. The ethics of footprinting in the context of privacy.

Keywords

Behavior – individual personal actions performed that are observable by third parties

Best Use (Policy) – explicit statement of the specific actions required in a given situation

Code of Conduct – documented rules outlining expected behaviors for an organization

Compliance – authenticated actions that indicate that a requirement, rule, or law is followed

Controls – a discrete set of human, or electronic, behaviors set to produce a given outcome

Critical Asset – a function, or object, that is so central to an operation that it cannot be lost

Cybercrime – antisocial acts committed using a computer, typically explicitly illegal acts.

Cyber law – formal legal system for adjudication of acts in cyberspace

Cybersecurity – assurance of confidentiality, integrity, and availability of information

Ethics – a standard for commonly accepted behavior in a given area of practice

Morality – a standard for commonly accepted correct behavior in a given culture

Norms – assurance of consistently correct behavior by individuals in the organization

Infrastructure – a collection of large components arrayed in a logical structure in order to accomplish a given purpose. Commonly used to describe the tangible elements of cyberspace.

Privacy – assurance that personally identifiable data is safeguarded from unauthorized access

Strategic Policy – the process of developing long-term plans of action aimed at furthering and enhancing organizational goals

References

Hurley, Deborah, “Improving Cybersecurity: The Diversity Imperative”, Forbes, CIO Network, 7 May 2017, www.forbes.com/sites/ciocentral/2017/05/07/improving-cybersecurity-the-diversity-imperative/#2f9e31c31e30, accessed March 2019.

Joint Task Force (JTF) on Cybersecurity Education, “Cybersecurity Curricula 2017, Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity, a Report in the Computing Curricula Series”, ACM/IEEE-CS/AIS SIGSEC/IFIP WG 11.8, Version 1.0, 31 December 2019.

Katyama, Fred, “Hacker Hits up to 8M Credit Cards, Secret Service and FBI Probe Security Breach of Visa, MasterCard, Amex and Discover Card Accounts”, CNN, 27 February 2003. https://money.cnn.com/2003/02/18/technology/creditcards/, accessed March 2019.

Microsoft Security Team, “The Emerging Era of Cyber Defense and Cybercrime”, Microsoft Secure. https://cloudblogs.microsoft.com/microsoftsecure/2016/01/27/the-emerging-era-of-cyber-defense-and-cybercrime/, 27 January 2016.

National Infrastructure Advisory Council (NIAC), “Surviving a Catastrophic Power Outage”, Department of Homeland Security, 11 December 2018.

Radware, “2018–2019 Global Application and Network Security Report,” 2019. www.radware.com/pleaseregister.aspx?returnurl=7563c321-ce21-4cc9-ae0d-4d75062acf70, accessed March 2019.

The Software Alliance, “Software Management: Security Imperative, Business Opportunity”,2018 BSA Global Software Survey, June 2018. https://gss.bsa.org/wp-content/uploads/2018/05/2018_BSA_GSS_Report_en.pdf, accessed March 2019.

The White House, National Strategy to Secure Cyberspace, February 2011.

Trend Micro, “Report on Cybersecurity and Critical Infrastructure in the Americas”, Organization of American States, Trend Micro Incorporated, 2015.

Index

A

B

C