INTERNAL AUDIT AND IT AUDIT SERIES

How to Build a Cyber-Resilient Organization

Dan Shoemaker • Anne Kohnke • Ken Sigler

CRC Press
Taylor & Francis Group
AN AUERBACH BOOK

How to Build a Cyber-Resilient Organization

Internal Audit and IT Audit

Series Editor:

Dan Swanson, Dan Swanson and Associates Ltd, Winnipeg, Manitoba, Canada

The *Internal Audit and IT Audit* series publishes leading-edge books on critical subjects facing audit executives as well as internal and IT audit practitioners. Key topics include Audit Leadership, Cybersecurity, Strategic Risk Management, Auditing Various IT Activities and Processes, Audit Management, and Operational Auditing.

Cognitive Hack: The New Battleground in Cybersecurity … the Human Mind
James Bone

Implementing Cybersecurity: A Guide to the National Institute of Standards and Technology Risk Management Framework
Anne Kohnke, Ken Sigler, and Dan Shoemaker

The CISO Journey: Life Lessons and Concepts to Accelerate Your Professional Development
Eugene M. Fredriksen

Data Analytics for Internal Auditors
Richard E. Cascarino

Practitioner's Guide to Business Impact Analysis
Priti Sikdar

Why CISOs Fail: The Missing Link in Security Management—and How to Fix It
Barak Engel

Supply Chain Risk Management: Applying Secure Acquisition Principles to Ensure a Trusted Technology Product
Ken Sigler, Dan Shoemaker, and Anne Kohnke

Project Management Capability Assessment: Performing ISO 33000-Based Capability Assessments of Project Management
Peter T. Davis and Barry D. Lewis

For more information about this series, please visit https://www.crcpress.com/Internal-Audit-and-IT-Audit/book-series/CRCINTAUDITA

How to Build a Cyber-Resilient Organization

Dan Shoemaker, Anne Kohnke, and Ken Sigler

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
AN AUERBACH BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed on acid-free paper

International Standard Book Number-13: 978-1-138-55819-9 (Paperback)

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

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

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

Contents

Foreword

The goal of a cybersecurity strategy is to prevent the compromise of resources. Attackers attempt to compromise networks, computers, and other resources by finding weak points in the cybersecurity policy, mechanisms, or strategy. The points at which they can reach the target system is called the *attack surface*. Cybersecurity policies and mechanisms aim to secure this surface.

Cyber resilience, as defined in this book, is a strategy to minimize this surface, and so make it less onerous to protect. It asks what the enterprise *needs* to protect to continue functioning successfully. Once these critical assets are identified, the architecture of the system is developed in such a way as to ensure that defenses protecting these assets are in place and effective. The rest of the enterprise can then be secured. The advantage of this asset-based approach is that the enterprise knows what assets it needs to protect, to what degree the protection must succeed, and what will happen should those protections fail.

It also aids in developing recovery mechanisms should those protections fail. In its traditional sense, "resilience" implies that the system may degrade, but it will recover. Here, given the knowledge of the critical assets, the enterprise can take steps to ensure that the system architecture keeps at least some of the asset available and functioning, even if not at the peak level, until the compromise is dealt with. Business functionality may be degraded for a time, but it will recover.

Developing a cyber-resilient plan requires both risk analysis and planning. First, the risk analysis shows what will happen when assets become compromised or fail. The enterprise and its stakeholders then determine what is acceptable to them—and, more importantly, what is not. This identifies the critical business functionality of the enterprise, and from that the critical assets can be identified. The cost of failure can be prioritized, giving an ordering of the critical assets. This enables the enterprise to deploy its protective resources to its greatest benefit.

The idea of beginning with the critical assets runs counter to the way much cybersecurity is done. Generally, the attack surface of the system is defined by examining possibly the entire system, locating points of potential weaknesses, and monitoring or strengthening them. The problem with using *only* this approach is twofold. First, the attack surface defined in this way is very broad. Second, the attack surface covers both critical and noncritical assets *without distinction*. This last point is particularly important, as the enterprise might protect something very well that, when it is compromised, does little to no damage to the business of the enterprise, and not protect something very well that, when it is compromised, disrupts the business function of the enterprise. Its lack of discrimination of criticality may result in the enterprise allocating its protection resources inappropriately.

Perhaps even more important is the need to locate the assets, understand them and how they play into the mission of the enterprise, and what the cybersecurity policy relevant to that asset should be. All too often, institutions lose track of assets or fail to understand how the functionality of one asset affects another asset. The risk analysis and prioritization needed to develop a cyber resilience strategy as discussed in this book will, if done correctly, ensure that the enterprise knows what its critical assets are, how they affect one another, what the requirements of the policy are in order to "secure the asset," and how that policy should be implemented.

This book presents a methodology for developing a cyber resilience strategy. It will aid enterprises in securing their resources. Thus, it fills a need, and fills it very well.

Matt Bishop
Davis, CA
July 12, 2018

Preface

You Can't Secure Everything

Persistent threats are so all-encompassing in the virtual ecosystem that it is unrealistic to think that you can defend against all of them. This means that successful cyberattacks will occur, no matter how much money we throw at the problem. So, organizations need to adopt a strategy that will ensure that its critical assets are protected, no matter what other items are compromised. The aim of this text is to present a novel new approach that has been devised to do that very thing.

At present, we secure systems at all logical points of access. Even defense-in-depth schemes simply involve the creation of increasingly rigorous perimeters. This new approach makes the practical assumption that instead of defending assets at all points of access, the organization ensures that only the things that the organization simply can't live without are unconditionally protected.

In concept, this strategy would narrow the protection scheme to the point where absolute assurance could be guaranteed for only some items while reducing the impact and recovery time of the rest of the organization's noncritical assets. This selective versus universal approach to security has been termed "cyber resilience."

Why Cyber Resilience?

Cyber resilience has a much narrower focus than cybersecurity. At its heart, cybersecurity concentrates a targeted set of protection measures on every viable point of access. Because there are a lot of potential access points, a cybersecurity solution requires a very large resource commitment.

Cyber resilience focuses on identifying and locking down just those assets that the organization needs to ensure the survival of the business. Then, cyber resilience conducts a disciplined recovery process that ensures the timely restoration of its noncritical assets to an acceptable level of operation, with the minimum amount of harm.

The concept of cyber resilience is supported by three of Saltzer and Schroeder's lesser-known principles.

1. *Economy of mechanism*: Keep the design as simple and small as possible.
2. *Least common mechanism*: Minimize the amount of mechanism common to all users.
3. *Work factor*: The cost must be greater than the potential attacker is willing to commit.

These principles make the cyber resilience concept more effective and less resource intensive than other approaches. Economy of mechanism locks up just the critical assets. This allows for simplicity in the design and implementation of the protection. It also concentrates resources on ensuring the protection of the critical assets rather than diffusing the investment across all assets. Most importantly, if the protection of the critical asset is made robust enough, attacking it will become too expensive and time consuming for the attacker, forcing them to move to more vulnerable targets.

Purpose of the Text

You will learn how to create a verifiable cyber-resilient infrastructure, which will ensure reliable security for critical objects. The book will explain how to establish systematic identification, prioritization, protection, and recovery processes. This is embodied in seven generic principles:

1. *Classify*: You can't protect things that you don't know exist. Thus, all the organization's assets must be identified, labeled, and arrayed in a coherent baseline of "things."
2. *Risk*: Resiliency requires appropriate situational awareness. Therefore, all known threat scenarios as they apply to the identified asset base must be identified and evaluated.
3. *Rank*: The assets that the organization absolutely can't afford to lose are prioritized, and provably effective countermeasures are designed for each of the priority assets.
4. *Architecture*: Resilience is baked into the architecture through a targeted set of well-designed and practical controls.
5. *Test*: Architectural resilience is evaluated against stated mission goals.
6. *Recover*: Well-defined processes are established to ensure that all noncritical assets are fully restored within reasonable and effective parameters.
7. *Evolve*: The organization dynamically adjusts its cyber-resilient architecture based on lessons learned over time.

Organization of the Text

This book encapsulates the belief that the creation of a cyber-resilient architecture is a strategic exercise. The outcome of this exercise is a formally defined and implemented infrastructure of best practices specifically aimed at optimizing the survival of critical organizational functions across the organization. As with any complex process, deployment can only be substantiated through a rational and explicit framework of auditable controls. The process for creating and deploying those controls is what is presented in these chapters.

Chapter 1: It's Time for a New Paradigm

The book will detail the general process for creating a cyber-resilient organization. The goal of this chapter is to give the reader an understanding of the overall strategic concept of cyber resilience as well as provide the justification and advantages of cyber resilience as a practical method for assuring organizational survival.

Readers will see how fundamental strategic activities can provide the basis for the absolute assurance of the critical assets of an organization. Readers will understand the differences between cybersecurity and cyber resilience. They will see that the actions taken to ensure cyber resilience are more cost effective and likely to assure organizational survival. Finally, we will describe the strategic planning process for establishing cyber resilience in any organization.

The reader will learn why a formal, comprehensive methodology aimed at ensuring the safety and security of vital assets is critical to the success of a cyber-resilient architecture. The aim of this chapter is to give an overview of the typical process of cyber resilience strategic planning including the necessary associations that must be created between the steps in the process. To ensure cyber resilience, these steps must be fully planned and coordinated across the organization.

Coordination of this degree of complex design and sustainment work requires a common and coherent methodology. The methodology that we outline will give managers practical control over the establishment and operation of a cyber-resilient architecture. The aim of this chapter is to provide readers with the ability to create and operate a cyber-resilient organization.

Chapter 2: Asset Identification and Classification

In some respects, cyber resilience is nothing more than an ultimate defense-in-depth and continuity management solution rolled into a highly focused protection mission. The core aim of cyber resilience is to maintain critical business functionality at all costs. Thus, the decisions that come out of the cyber resilience design process will determine how the business will invest its precious time and resources and build its architecture.

The key to cyber resilience lies in understanding what constitutes core functionality. Cyber resilience assumes that all systems will eventually be compromised. Given this assumption, the cyber resilience function ensures a robust array of specifically targeted controls to ensure that only the subset of functions essential to the continuing operation of the business are fully and completely protected, even if all other system activities are compromised.

In conjunction with the aim of ensuring the survival of core functionality, the cyber resilience process also defines clear, straightforward, and practical paths to restore any lower priority functions that might have been lost in the actual compromise. The seven stages of cyber resilience are designed to achieve those two specific goals. The identification process is perhaps the most important step in creating a cyber-resilient organization. That is because the outcome of the classification process will drive every subsequent protection action.

Logically, if an organization does not understand what assets it has, it is almost impossible to intelligently protect them. Thus, a deliberate, formally executed, and documented classification activity is the key starting point. This is an organization-wide exercise whose aim is to understand the criticality, sensitivity, and priority of all items in the asset base. It involves all stakeholders because buy in is an essential condition for embedding changes in the organization.

Chapter 3: Establishing the Risk Status of the Corporate Infrastructure

Risk assessment provides timely and accurate understanding of the threat status of all components of the asset base, and is essentially a situational awareness function. The risk stage employs situational awareness practices to drive the decisions about the best way to ensure that critical assets and services will continue to function as desired. The aim is to fully understand every hazard in the threat environment that might affect a critical asset. The term "hazard" denotes a threat or an incident, natural or man-made, that warrants action to protect against harm and to minimize disruptions of the mission.

This includes natural disasters, cyber incidents, acts of terrorism, sabotage, and destructive criminal activities targeting critical components of the enterprise infrastructure.

The outcome of this phase is a detailed map of the risk environment sufficient to support decision-making with respect to organizational priorities. No decisions are made until the entire threat assessment is mapped. There is obviously a potential that meaningful threats might be missed or that a new threat might appear after the original risk assessment is completed.

Additionally, there should be a comprehensive plan to ensure subsequent systematic risk assessments against any potential attack that might occur against assets viewed as critical. Since the architecture will be altered to respond to those threats, it is also crucial that a process exists to rapidly respond to those risks. The outcome is reasonable confidence that all conceivable risks to a given asset and its dependencies have been identified, characterized, and ranked for likelihood and impact.

Chapter 4: Prioritization of Assets and Establishing a Plan for Resilient Change

This is the second most important aspect of the cyber resilience process. Once the organization's assets have been identified and baselined and the threat environment characterized, the criticality of all assets in the asset baseline is ranked. This is an organization-wide ranking process involving all stakeholders. "Assets" comprise all the people, processes, technologies, and facilities required to achieve the organizational purpose. However, some assets are more critical than others. The ranking process identifies, documents, and assures only those assets ranked as "critical" to the organization's mission, vision, values, and purposes.

Unfortunately, ranking can often turn into a political free-for-all where various stakeholders attempt to enforce their own agendas. Obviously, this can't be allowed to happen if the eventual architectural solution is going to be truly resilient. Therefore, criticality must be understood based on a clear map of functions and dependencies, which are referenced in an objective and rational way to the mission and goals of the organization. This chapter will discuss how an asset can only be labeled "critical" if it provably underwrites some aspect of the organization's core functionality.

A rigorous set of protection requirements are specified for just those assets that directly enable the organizational mission. Rigor is defined as the ability to resist any known or conceivable method of attack. Relevant stakeholders are assigned to supervise and maintain each asset. Effective communication linkages are established between those stakeholders and documented. Then the protection requirements, access links, and the requisite permissions are enabled as a coherent set of electronic and behavioral controls. This includes methods for initiating, planning, executing, and following up/remediating active behaviors for the purposes of systematic control. It also includes the definition and assignment of all roles and responsibilities for every participant in the supply chain, customer, supplier, and integrator. It also includes the best practices for documentation and reporting of control information to appropriate sources.

Chapter 5: Control Design and Deployment

The only way to ensure proper implementation of a critical process is through design. Design deploys the controls required to ensure a critical asset. This is a strategic governance activity. Design creates an infrastructure of substantive controls to effectively satisfy its stated mission, goals, and objectives. Therefore, this phase identifies the explicit control objectives for each critical asset.

The architectural development process prioritizes those objectives and implements targeted control actions to most effectively achieve priority objectives. Then it analyzes and assesses the deployed control set to ensure that the resultant infrastructure satisfies the critical purpose. If documented control objectives are not satisfied, this process undertakes the necessary analysis to modify controls or plug gaps.

Chapter 6: Control Assessment and Assurance

Cyber resilience must be assured. This is a testing and assurance function that characterizes the explicit level of control performance against the protection goals. The intention is to be able to say with assurance that the aggregate controls for any given acquisition are effective given the aims of the organization.

Operationally, this should take place within a defined reporting and decision-making structure. This is an assessment process comparable to the systematic monitoring and adjustment processes that most organizations employ to assure the effective performance of its functions. Because the overall purpose of assurance is to produce a trustworthy assurance outcome, the outcome of the Assurance and Evolution phase is continuous assurance of process correctness.

Chapter 7: Recovering the Non-Priority Assets

Organizations need to understand how resilient its critical services are. This is essentially the continuity management principle. The goal of recovery planning is to ease the impact of disruptive events by using well-established plans to ensure predictable and consistent continuity of the critical services. To do this, the critical service's operating environment is studied to identify all potential failure modes, and then a proper strategy to recover from all possible breakdowns or disruptions is devised.

The goal is to create a complete and consistent recovery process that will address all conceivable types of system compromise. The plan for incident recovery must be explicit for every asset, and lessons learned are compiled to develop improvement strategies. This requires an operational plan capable of identifying, analyzing, responding to, escalating, and learning from all adverse incidents in addition to a well-defined process for assigning roles and responsibilities and managing and tracking resolutions.

Chapter 8: Ensuring a Continuously Cyber-Resilient Organization

The goal of recovery planning is to ease the impact of disruptive events by using well-established plans to ensure predictable and consistent continuity of the critical services. This is essentially the continuity management principle. Organizations need to maintain the assured functioning of all its services. This is an infrastructure evolution process.

To do this correctly, the critical service's operating environment is studied to identify all potential failure modes, and then a proper strategy to recover from all possible breakdowns or disruptions is devised. The goal is to create a complete and consistent infrastructure of controls that will achieve the purposes of cyber resilience.

The plan for development of this infrastructure must be explicit for every asset, and lessons learned are compiled to develop improvement strategies. This requires an operational plan capable of identifying, analyzing, responding to, escalating, and learning from all adverse incidents.

Expectations

This book presents an approach that is meant to implement a state of cyber resilience as a real-world condition. This is a business-level activity. Therefore, there are no expectations about specialized technical knowledge. All readers will learn how to design and evolve a cyber-resilient architectural process for a given organization as well as how to maintain a state of cyber resilience in the day-to-day operation of the business. After reading this, the reader will know how to ensure a stable state of systematic cyber resilience within their organization as well as evolve the protection scheme to continue to appropriately address the threat environment.

At the end of this book, the reader will be able to

1. create, sustain, and evolve a cyber-resilient organizational infrastructure;
2. define and evaluate control arrays to ensure all assets of critical value;
3. ensure full and complete recovery of noncritical assets in the timeliest and most effective way possible.

Authors

Dan Shoemaker, PhD, is principal investigator and senior research scientist at the University of Detroit Mercy (UDM) Center for Cyber Security and Intelligence Studies. Dan has served 30 years as a professor at UDM, with 25 of those years as department chair. He served as a cochair for both the Workforce Training and Education and the Software and Supply Chain Assurance Initiatives for the Department of Homeland Security, and was a subject matter expert for the National Initiative for Cybersecurity Education (NICE) Workforce Framework 2.0. Dan has coauthored seven books in the field of cybersecurity and has authored over one hundred journal publications. Dan earned his PhD from the University of Michigan.

Anne Kohnke, PhD, is an Associate Professor of Information Technology at Lawrence Technological University. After a 25-year career in IT, Anne transitioned from a Vice President of IT and Chief Information Security Officer (CISO) position into full-time academia in 2011. Anne's research is focused in the area of cybersecurity, risk management, threat modeling, and mitigating attack vectors. Anne received her PhD from Benedictine University, and has coauthored four other books in the cybersecurity discipline.

Ken Sigler is a faculty member of the Computer Information Systems (CIS) program at the Auburn Hills campus of Oakland Community College in Michigan. His primary research is in the areas of software management, software assurance, and cloud computing. He developed the college's CIS program option entitled "Information Technologies for Homeland Security." Until 2007, Ken served as the liaison for the college to the International Cybersecurity Education Coalition (ICSEC), of which he is one of three founding members. Ken is a member of IEEE, the Distributed Management Task Force (DMTF), and the Association for Information Systems (AIS).

Chapter 1

It's Time for a New Paradigm

Following this chapter, the reader will understand

1. the role and importance of cyber resilience in protecting organizations;
2. the differences between cybersecurity and cyber resilience;
3. the standard steps of the cyber-resilient approach;
4. the concerns and issues associated with our cybersecurity;
5. the general structure and intent of a cyber-resilient architecture;
6. the large steps to implement formal cyber-resilient processes.

Introduction to the Book

Two decades of data make it clear that conventional cybersecurity doesn't work (Symantec, 2014; Trend-Micro, 2015; PRC, 2016). Hence, this book offers an entirely new and different approach, one that is both resource efficient and one which ensures that the organization will continue to survive, no matter how destructive the attack. We call this approach "cyber resilience." Cyber resilience is not the same thing as cybersecurity. Cyber resilience ensures the absolute protection of just those functions that are vital to the organization's survival.

This chapter will introduce the general principles and concepts of cyber resilience as well as the standard methodology and contextual activities that guide the implementation of a strategically sound cyber-resilient architecture. We will detail the fundamental phases involved and the best practices that must be implemented in each of the phases of a classic cyber resilience process. These phases build upon each other in a collective fashion and proper execution of each is integral to the assurance of organizational resiliency.

Organizational resilience is important because the increasing presence of advanced cyber threats makes it inevitable that every organization will ultimately be targeted (OAS, 2015). Cyber resilience recognizes that there are too many cutting-edge hacking tools to prevent sophisticated attackers from finding the cracks in even the most robust cybersecurity perimeter (Lois, 2015). Thus, there is a need for a new paradigm.

Cyber resilience requires the organization to spend whatever it takes to develop a well-defined and explicit set of controls to ensure the survival of just those critical elements that cannot be subjected to compromise. The controls must assure provable protection of core functionality and the various interdependencies in the enterprise's ecosystem (EY, 2014). The concept of cyber resilience goes far beyond the classic boundaries of better access controls (EY, 2014). Instead, organizations establish a "cyber resilience strategy and architecture" that give them the ability to withstand and recover rapidly from disruptive events (EY, 2014).

Practically speaking, the best argument for cyber resilience is that it concentrates resources where they will make the most difference. This is particularly germane to national security in that any attack on an infrastructure element threatens a lot more than simple business processes (Conklin, Shoemaker, Kohnke, 2017). Thus, cyber resilience is a particularly significant aspect of ensuring survival and easing recovery of the critical systems that underwrite our way of life.

In general, it is our belief that very little substantive thinking has taken place when it comes to devising a specific and generally reliable approach to protecting the nation's critical infrastructure. This is partly because there is no practical process that explicitly dictates how to reliably protect critical infrastructure components. The ideas presented here are a start toward eventually overcoming this lack of planning.

Readers will understand the ultimate reasons why cyber resilience provides more robust assurance for the organization. They will also discover the role that conventional strategic management plays in the creation and maintenance of an effective cyber-resilient architecture. Finally, the last chapter of this book will describe the practical means for operating an organization in a cyber-resilient state.

Why Cyber Resilience Is Critically Important

Count on it—the next world war is going to start with the click of a mouse, not a wave of bombers. The attacker will send a command to the computers that control key elements of our critical infrastructure, and most of our way of life will be blasted back to the 18th century. Could this really happen? Two decades of data say that it is not only possible, but that it will indeed take place. In fact, we have struggled with this problem almost from the beginning of the internet. But the trend is always in one direction: "One massive hack after another" (Gamer, 2015). Worse, data indicates that conventional cybersecurity approaches will never be able to successfully protect us (Symantec, 2014; Trend-Micro, 2015, PRC, 2016).

Cyberspace is full of adversaries. Potential actors range from state-sponsored groups through criminal enterprises to any wacko with an internet link. So, cyberattacks on the various elements of the U.S. critical infrastructure are a daily fact of life. For instance, the Industrial Control Systems-Computer Emergency Response Team (ICS-CERT) reports that U.S. industrial control systems were attacked at least 245 times over a 12-month period (OAS, 2015). "While China, the U.S. and Russia lead the world in cyber-attacks, virtually every government engages in such attacks, and nearly every country has its share of computer hackers" (Wagner, 2017). So, forget aircraft carriers, the ability to launch a successful cyberattack makes every nation-state into a potential superpower (Wagner, 2017).

So far, the problems have been elsewhere. Perhaps the most egregious example comes from Ukraine. In December 2015, a presumed Russian cyberattacker successfully seized control of the Prykarpattyaoblenergo Control Center (PCC) in the Ivano-Frankivsk region of Western Ukraine (Wagner, 2017). The attack marked the first time that a concerted cyberattack was successfully launched against a nation's power grid (Wagner, 2017). However, Stuxnet, in 2010, might be the first instance of "a nation enforcing policy through other means," to paraphrase Von Clausewitz (Clausewitz, Chapter 1, Section 4, 1976).

Worse, the perpetrators of the Ukrainian attack were observed conducting similar exploits against the U.S. energy sector (Brasso, 2016). Although there was never any actual disruption, many experts believe that those activities were a probe for future moves on the U.S. infrastructure (Brasso, 2016). Consequently, in the larger sense, the key question is "could a catastrophic cyberattack in the U.S. infrastructure ever occur?" The National Security Agency's former Director, Mike Rodgers, made his own evaluation of the possibility of a successful attack against critical infrastructure when he said: "it's a matter of, when, not if" (Smith, 2014).

Power grids are the most frequently mentioned targets (Wagner, 2016; Brasso, 2016; Smith, 2014). This is because the interconnectedness of power grids opens them up to "cascading failures." That is, as nearby grids take up the slack for a failed grid system, they overload and fail themselves and cause a chain reaction. Rogers says that such attacks are part of "coming trends" in which so-called zero-day vulnerabilities in U.S. cyber systems are exploited (Smith, 2014).

The reason why the protection of our national infrastructure is so critically important is that a major exploit, like a successful cyberattack on the electrical grid, could leave the U.S. cloaked in darkness, unable to communicate and without any form of 21st century transport. It would likely kill many thousands of citizens, perhaps millions, either through civil unrest, failure of public systems, or mass starvation (Brasso, 2016; Maynor and Graham, 2006).

Many experts believe that the cyberwar began in 2003 (Wagner, 2017). This was when the Northeast (U.S.) blackout occurred and caused 11 deaths and an estimated

$6 billion in economic damages (Wagner, 2017). After that attack, SCADA (supervisory control and data acquisition) attacks occurred in the UK, Italy, and Malta, among others. According to Dell's 2015 Annual Security Report, cyberattacks against infrastructure systems doubled in 2014 to more than 160,000 (Wagner, 2017).

Infrastructure Is the Target

Infrastructure systems are diverse. This diversity and the criticality of the sensors and controllers that comprise a typical infrastructure system make them tempting targets for attack. Therefore, there have been long-standing concerns about the overall digital infrastructure being vulnerable to cyberwarfare and cyberterrorism attacks (Eisenhauer et al., 2006; Nat-Geo, 2017). Nevertheless, notwithstanding the disastrous nature of cyberattacks on digital targets, none of the industries in our current national infrastructure have developed coherent plans or effective strategies to protect themselves (Brasso, 2016). This is the reason why there is increasing interest in a coherent model for defending the critical infrastructure against cyberattack (Symantec, 2014; EY, 2014).

The approach we are going to discuss here is particularly suited to ensuring the continuing survivability of infrastructure systems. This is because the focus is on maintaining core functionality rather than protecting data. The idea is to only lightly defend less critical or peripheral elements while ensuring the survival of the system. This strict emphasis on survivability versus data protection is the reason why cyber resilience, versus cybersecurity, is the approach of choice for critical systems.

A New Paradigm for Ensuring Our Way of Life

This book offers an entirely new and different paradigm. Cyber resilience ensures the absolute security and reliability of just those critical functions, which the organization needs to continue to survive and carry out its mission. Carl von Clausewitz sums up the role of strategy in this way: "Strategy is the necessary response to the inescapable reality of limited resources" (Clausewitz, 1989). In short, no General ever has the luxury of overwhelming numbers or unlimited resources. So, s/he needs to adopt an approach that is likely to succeed, given the assets that are available at the time of battle. In this respect, Clausewitz posits that a successful strategy finds the most advantageous point to concentrate all the resources necessary to achieve the primary goal, which is to win the battle even if some of the lesser objectives are not achieved (Clausewitz, 1989).

Cybersecurity is the inheritor of the old information assurance mission. Accordingly, cybersecurity is still based around creating and ensuring a protection perimeter. This perimeter is shaped by assuring all logical points of access to the protected space that lies within that boundary. Since the protection perimeter of even a small organization can involve numerous points of access, electronic, physical and human, that task normally requires an extensive resource commitment to be even be remotely successful.

Whereas, cyber resilience only ensures those organization elements that are deemed critical to system survival. The requirement to maintain the functioning of a few critical components is less resource intensive than the need to ensure the confidentiality, integrity, and availability of all assets within secure space. Therefore, cyber resilience is much more resource efficient. The narrowing of scope allows protection measures to be concentrated onto a far smaller attack surface, which notionally ensures more effective protection for the things that simply can't be allowed to fail.

Operationalizing Cyber Resilience: Saltzer and Schroeder's Principles

Cyber resilience is founded on classification, prioritization, and comprehensive strategic policy-based deployment of a rigorous set of real-world security controls (Symantec, 2014). Cyber resilience requires the creation of a set of well-defined processes, which react to penetrations of the organizational perimeter by locking down the asset they are designed to protect (US-CERT, 2016). These protection processes are both electronic and behavioral in focus and they are designed to protect key assets as well as ensure optimum recovery of the overall system in the event of successful attack (Symantec, 2014).

Saltzer and Schroeder arguably laid down the basis for cybersecurity design in their founding principles (Saltzer, 1974). The concept of cyber resilience hinges on four of Saltzer and Schroeder's lesser-known principles. Most people in cybersecurity know about and practice design concepts such as Least Privilege, Complete Mediation, Separation of Duties, and Psychological Acceptability. Figure 1.1 lists four principles that are generally not as prevalent and underlie the cyber resilience approach (Saltzer, 1974):

1. *Economy of mechanism*: Keep the design as simple and small as possible.
2. *Work factor*: The cost must be greater than the potential attacker is willing to commit.
3. *Least common mechanism*: Minimize the amount of mechanism common to all users.
4. *Compromise recording*: Reliably record the actions of a compromise.

Economy of mechanism advises the construction of simple strongpoints around critical assets rather than basing the protection on the complexities of comprehensive

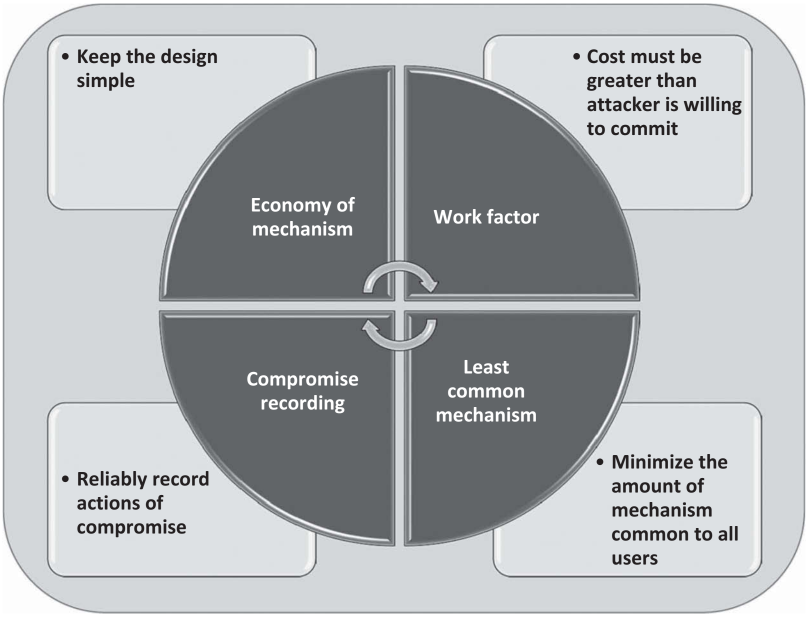
• Keep the design simple
• Cost must be greater than attacker is willing to commit
Economy of mechanism
Work factor
Compromise recording
Least common mechanism
• Reliably record actions of compromise
• Minimize the amount of mechanism common to all users

Figure 1.1 Saltzer and Schroeder's lesser-known cyber principles.

perimeter access control. In conventional military tactics, a strongpoint is a key position, which is very difficult to overrun or avoid. With respect to illustrating the difference between cyber resilience and cybersecurity, perhaps the best practical example would be that a strongpoint is like locking critical assets in a safe rather than protecting them by assuring access to the building they are in, which is perimeter access control.

In military doctrine, strongpoints are arrayed in mutually supporting, defense-in-depth mesh arrangements, called hedgehogs, rather than formed into a contiguous line of increasingly rigorous perimeter access controls. The hedgehog arrangement implements the principle of *least common mechanism* in that strongpoint defenses are tailored to just the threats affecting the protection target. This allows for very straightforward simplicity in the design. It also allows the organization to maximize security resources by building up the capabilities of only the protection for the critical features rather than diffusing the investment by attempting to protect everything.

Most importantly, if the strongpoint protecting the critical assets are robust enough, they will be too expensive for the attacker to assault. So, the attacker will be shepherded to more vulnerable targets and that brings us to the work factor principle in operation.

Work factor also serves to maximize the defender's rapid response capability. In effect, organizations will be able to rapidly concentrate their resources at the point of attack, knowing that the essential functions are protected. Since the critical system protection, e.g., strongpoint positions, will be bypassed due to their impossibly high work factor rate, the organization will be able to concentrate its resources on the recovery of noncritical functions and information.

Finally, the organization will be able to deploy and conduct the most effective recovery possible because information from prior incidents will be available to planners and responders to help optimize the response. This is the intent of the *compromise recording* principle. The effect of an attack on a nonessential resource can be minimized through lessons learned from prior attacks. Additionally, the road to recovery can be planned because the execution and outcomes of the attack have been recorded for study.

Tactics One and Two: Economy of Mechanism and Work Factor

Cyber resilience involves the formulation of well-defined strategies and the implementation of rigorous strongpoint countermeasures, which are designed to inflict unsustainable work factor requirements on an attacker. Consequently, the most important thing the organization needs to know is: "Exactly how many strongpoints will I need to build and exactly how much investment will be required to make each strongpoint infeasible to attack?" It should be possible to identify all those organizational functions that are too critical for the organization to lose and still stay in business. This involves a strategic planning process and accordingly, the organization should then concentrate sufficient resources to ensure that those specific protection targets always demand too great an investment on the attacker's part. Thus, cyber-resilient architectures are founded on making decisions about what that organization can't afford to lose and then ensuring that it doesn't lose them.

The success of a cyber-resilient defense hinges on defining protections for critical assets that are too costly for the attacker to break. These protections don't have to ensure absolute and unquestionable security, but they DO have to assure enough protection that attackers will find the resource investment unpalatable, and thus move on to another target. Since there is likely to be a much greater number of soft targets, e.g., nonessential assets versus hard ones, cyber resilience defenses will not require as great an investment as a strategy that is aimed at protecting all the resources, soft and hard, inside a perimeter.

Tactic Three: Least Common Mechanism

To implement a proper strongpoint defense, the relationship between the system's critical assets must be identified and labeled. This is necessary to establish the precise state of dependencies and interdependence of objects within the system. More importantly, the interface between the users of those assets must be well understood and characterized to implement control. Next, a broad-spectrum risk assessment ought to be performed for each of the identified system interdependencies and user accesses. The idea is to obtain full situational awareness, both in terms of critical asset interactions as well as the potential threats arising from them. Using the full situational awareness, a provably effective control response must be deployed for each of the critical assets. Resources are focused on assuring only those components that are designated as critical. This is primarily an engineering design exercise, driven by precise knowledge of the components and their interrelationships. The resources that are left over after all critical asset dependencies are ensured are then allocated to protection and recovery of the rest of the system.

Since no single function operates separately from all the other critical functions, the resilience must be baked into the architecture in such a way that critical functions cannot be accessed by a backdoor. This is a pure design/control deployment exercise. Nevertheless, resilience of the critical asset control design and deployment needs to be confirmed correct. This is a classic testing and assurance function that periodically characterizes the effectiveness of critical control performance against stated mission goals.

Tactic Four: Compromise Recording and Strategic Recovery Planning

Well-defined processes need to be established to ensure that all data obtained from both attacks and compromises is recorded for analysis and planning. The aim is to ensure that all system functions are fully restored within requisite parameters, based on a method or plan. This requires a suitable array of evidence gathering review and testing processes and metrics sufficient to evaluate any form of compromise for future planning (Bradford, 2017).

The aim is to allow the organization to wholly understand its digital environment. This allows it to build the most effective rapid response team and design well-defined scenarios for how each attack will be managed. The main reason why compromise recording is so effective is that 98% of cybersecurity incidents fall into nine basic attack patterns (Verizon, 2018) as shown in Figure 1.2:

1. Denial of Service
2. Privilege Misuse
3. Crimeware
4. Web App Attacks
5. Physical Theft and Loss
6. Miscellaneous Errors
7. Cyber-Espionage
8. Point of Sale
9. Payment Card Skimmers

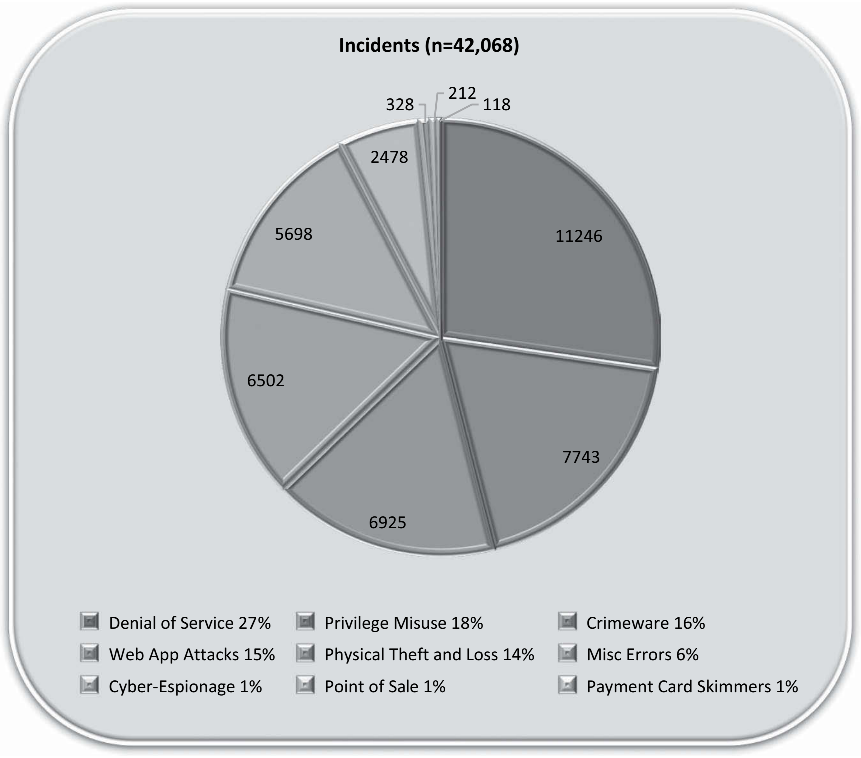

Figure 1.2 Percentage and count of incidents per classification attack patterns.

These basic attack patterns can be studied, documented, and a response can be crafted to ensure the most effective resolution for a given known situation. The ability to dynamically respond to exploits, based on lessons learned, is crucial to keeping costs down. If this is done correctly, the organization will have both security and cost efficiency.

Cyber Resilience versus Cybersecurity

The underlying assumption is that redesigning or updating the organization to a cyber-resilient architecture will make attacks on organizational functions less likely to succeed. In addition, the architecture will minimize the consequences of cyberattacks when they do succeed, increase costs and uncertainty for the adversary, and possibly act as a deterrent against future attacks. Thus, cyber-resilient organizations can "tough-out" the types of assaults that bring conventionally protected organizations to their knees.