Chris K. Williams, Scott E. Donaldson, and Stanley G. Siegel
Building an Effective Security Program

Chris K. Williams, Scott E. Donaldson,
and Stanley G. Siegel

Building an Effective Security Program

DE GRUYTER

ISBN 978-1-5015-1524-8
e-ISBN (PDF) 978-1-5015-0652-9
e-ISBN (EPUB) 978-1-5015-0642-0

Library of Congress Control Number: 2020939274

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available on the Internet at http://dnb.dnb.de.

Cover image: maxkabakov/iStock/Getty Images Plus
Typesetting: Integra Software Services Pvt. Ltd.
Printing and binding: CPI books GmbH, Leck

www.degruyter.com

This book is dedicated to the memory of our colleague, beloved friend, and scholar, Stanley G. Siegel. Stan's keen intellect, perceptive questioning, and kind-heartedness educated many, and inspired all who knew him.

Scott E. Donaldson
Chris K. Williams

Acknowledgments

No book project can be accomplished successfully without some impact on home life. To our families, we express our gratitude for their patience while we spent countless evenings and weekends away from them writing this book. Because this time can never be reclaimed, we are forever grateful for their understanding and support.

We thank De Gruyter, and Jeff Pepper for accepting this project and mentoring us through the authorship process. We thank Jaya Dalal for her careful review of our material at each stage of the process. We thank Natalie Jones for helping us convey our thoughts in clear and unambiguous terms, and correcting us when we went awry. We thank André Horn and his team for their professional management of this complex and challenging project.

Finally, we thank our reviewers and friends who took time from their busy schedules to review, comment, listen, and advise on our content and ideas. Your inputs made our ideas better than they were before, and for that service we are forever in your debt.

— Scott Donaldson, Chris Williams, Stan Siegel

https://doi.org/10.1515/9781501506529-202

About the Authors

Chris K. Williams has been involved in the cybersecurity field since 1994 in a combination of U.S. military and commercial positions. He has been in the cybersecurity field for more than 20 years focusing on enterprise cybersecurity strategy, architecture, and compliance. He is a veteran of the U.S. Army, having served five years as an airborne paratrooper in Fort Bragg, NC. He has worked on cybersecurity projects with the U.S. Army, Defense Information Systems Agency, Department of State, Defense Intelligence Agency, and numerous other commercial and government organizations. He focuses on designing integrated solutions to protect against modern threats.

Williams co-authored *Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats* (Apress, 2015) and its companion book *Enterprise Cybersecurity: Study Guide* (Apress, 2018). He also co-authored *Understanding Security Issues* (Walter de Gruyter Inc., 2019). He holds a patent for e-commerce technology, and has published technical papers with the Institute of Electrical and Electronics Engineers (IEEE) and other publications. He has presented on cybersecurity at RSA, Milcom, the International Information Systems Security Certification Consortium $(ISC)^2$, the Information Systems Security Association (ISSA), and other forums.

Williams holds a BSE in Computer Science Engineering from Princeton University and an MS in Information Assurance from George Washington University.

Scott E. Donaldson has professional experience in the defense, federal, commercial, and university marketplaces. His expertise includes software systems development, information technology, cybersecurity, and multi-hundred-million-dollar program management. He has served in a wide variety of technical and management leadership roles including chief technology officer, chief information officer, chief systems engineer, and senior program manager.

Donaldson has co-authored seven books including *Understanding Security Issues* (Walter de Gruyter Inc., 2019); *Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats* (Apress, 2015); and *Successful Software* De*velopment: Making It Happen*, 2nd Edition (Prentice Hall PTR, 2001).

He has also contributed to other software engineering books: *Encyclopedia of Software Engineering*: *Project Management – Success Factors (Reducing the Likelihood of Software Failures)* (CRC Press, 2010) and the *Handbook of Software Quality Assurance: Software Configuration Management – A Practical Look*, 3rd Edition (Prentice Hall, 1999).

Donaldson has a BS in Operations Research from the United States Naval Academy and an MS in Systems Management from the University of Southern California. He teaches graduate courses in software systems engineering at Johns Hopkins University, which honored him in 2009 with an Excellence in Teaching Award.

https://doi.org/10.1515/9781501506529-203

Dr. Stanley G. Siegel's professional experience included senior-level positions as a systems engineer, mathematician, and computer specialist. He started his career with the U.S. Government in the Department of Commerce and then the Department of Defense. After his government service, he was with Grumman for 15 years and Science Applications International Corporation (SAIC) for over 20 years. He helped SAIC grow to an $11 billion leader in scientific, engineering, and technical solutions with hundreds of millions of dollars in new business.

Siegel earned a nuclear physics doctorate from Rutgers University. While at SAIC, he served as a senior technical advisor and director on a wide spectrum of projects in areas such as software engineering methodology assessment, software requirements analysis, software testing and quality assurance, and technology assessment.

He and Donaldson jointly taught graduate courses since the mid-1990s. They taught both in-class and online software systems engineering courses at Johns Hopkins University Whiting School of Engineering. Johns Hopkins honored them in 2009 with an Excellence in Teaching Award.

Siegel co-authored four software engineering books including the seminal textbook *Software Configuration Management: An Investment in Product Integrity* (Prentice Hall, 1980) and *Successful Software Development: Making It Happen*, 2nd Edition (Prentice Hall PTR, 2001). He co-authored *Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats* (Apress, 2015) that empowers organizations to defend themselves against the threat of modern targeted cyberattacks. He also co-authored *Understanding Security Issues* (Walter de Gruyter Inc., 2019) that helps people protect their digital life at work, at home, and on travel.

He contributed to a number of books, including the *Encyclopedia of Software Engineering, Software Project Management Success Factors (Reducing the Likelihood of Software Failures)* (CRC Press, 2010); and the *Handbook of Software Quality Assurance*, *Software Configuration Management – A Practical Look*, 3rd Edition (Prentice Hall, 1999).

Contents

Introduction

Computers, the internet, mobile computing, cloud, internet of things (IoT), and remote computing are transforming how we live and work every day. Internet technologies have opened up entirely new business sectors for entertainment, communication, collaboration, advertising, medicine, recruiting, travel, publishing, and product delivery.

Using these technologies, global teams can now collaborate worldwide in real-time, and permit hundreds, thousands, or even millions of people to simultaneously share knowledge and experience. Internet technologies enable employees of "virtual businesses" to collaborate and deliver value without ever actually meeting face-to-face. By tearing down obstacles to information sharing and dissemination, internet technologies have reduced costs and accelerated business solution delivery.

However, this transformation introduces its own sets of challenges and new risks to organizations, businesses, and people. Thanks to these new technologies and globally connected networks, the "bad guys" can use the internet to access thousands of computers, millions of accounts, and terabytes or petabytes of data – with only a few keystrokes or clicks. And that is not all that is at stake.

Over the past three decades, cyberattacks have destroyed computers, disrupted international trade, and resulted in billions of dollars in damage. Organized crime, hacktivists, corporate competitors, foreign adversaries, and countries have been incredibly successful at using compromised computers to carry out their cyberattacks. The daily lives of millions of individuals have been disrupted, as well as daily operations of organizations and governments around the world. Ransomware has disrupted entire businesses, multinational corporations, and even municipalities. Imagine entire cities unable to deliver essential services because the city government's computers are all being held hostage by an attacker thousands of miles away. Data breaches have compromised personally identifiable information, protected health information, and personal financial information for millions of individuals and their families.

Cyberattacks, while their impacts may be considerable, can be managed. While "perfect" cybersecurity remains a bit of a pipe dream, "good enough" cybersecurity is achievable – even on a limited budget and with limited resources. Organizations can achieve practical, cost-effective cybersecurity that is effective against attackers ranging from casual hackers to determined nation-states. Cybersecurity is everyone's responsibility, but there are things organizations can do to protect themselves and their people from cyber threats, today.

This book is about how to protect an organization from the dangers of the internet, while taking advantage of the benefits of the internet to support the

https://doi.org/10.1515/9781501506529-205

organization's business objectives. This book describes the risks to an organization, its employees, partners, and customers. It explains how an organization can manage its cyber risks, and how it can train its people to be a part of the organization's successful risk management, while also protecting themselves, their families, their coworkers, and their friends.

About This Book

This book helps an organization protect its employees, external partners, customers, families, and friends. This protection is holistic, and extends to work, home, and travel. This book provides information on how to structure and operate an effective cybersecurity program that includes people, processes, technologies, security awareness, and training. It helps organizations answer the following cybersecurity questions:

- *How do cyber threats target my organization?*
- *How can my organization identify its cybersecurity risks?*
- *What do hackers and cyberattackers want from my organization?*
- *How do cyberattacks penetrate organization cyberdefenses?*
- *How do organizations make a business case for cyberdefense investment?*
- *What are the regulatory drivers for cyber protections?*
- *What should organizational cybersecurity policies look like?*
- *What technologies may be used for an organizational cyberdefense?*
- *What does it take to operate organizational cyberdefenses?*
- *What can an organization do to increase its employees' cyber awareness?*
- *What are the elements of a cyber training and awareness program?*
- *How can an organization measure its cyber performance?*
- *What happens when cyber failures occur?*
- *How will organizational cybersecurity be changing in the future?*

To help answer these questions, and to reduce an organization's cybersecurity risk, this book contains guidance on the following topics:

- An understanding of today's cyberthreats and the dangers they pose.
- Common cybersecurity attacks and how attackers target an organization.
- How to understand cyber risk and use good practices to manage it.
- Guidance for defining organization cybersecurity policy and procedures.
- Elements of organization cyberdefenses and their operations.
- Approaches for protecting employees, customers, partners, and their data.
- Strategies for training organization executives, IT professionals, security staff, specialists, and partners in good cybersecurity practices.

- Techniques for measuring cyber performance and handling failures.
- Future trends in cyberattacks and cyberdefenses.

Who Should Read This Book?

This book is intended for people interested in protecting organizational IT infrastructure and digital information from cyberattacks. Readers of this book include:

- *Leaders* who
  - Have oversight responsibility for securing their organizations, and the devices and accounts used at their organizations.
  - Want to improve their organizations' cybersecurity posture through policy, technology, security awareness, training, and operations.
- *Professionals* who
  - Establish or operate cyberdefense programs at their organizations.
  - Need to understand cyberthreats targeting their organizations and their people at work, at home, and on travel.
  - Need to understand how cyberattackers penetrate organizational defenses and how to counter those attacks.
  - Want to learn techniques to reduce their organizations' cyber risk.
- *IT professionals* who are responsible for ensuring information technology solutions have adequate cybersecurity while delivering value to the organization.
- *Educators* who teach at the undergraduate or graduate levels, and instructors who conduct security awareness workshops, seminars, or training classes.
- *Students* who are learning about business, information technology, or cybersecurity and who need to understand the challenges of delivering effective cybersecurity solutions.

Everyone can use the book's content to help understand organizational cybersecurity and the challenges in coordinating people to improve overall cyber awareness and performance. By improving cyber understanding and awareness, organizations can make cyberattacks and cybercrime more difficult.

Contents of This Book

This book is primarily concerned with cybersecurity for organizations, while also considering the technical elements that make up organizational cyberattacks and cyberdefenses. The book chapters are meant to be read in sequence, as they

build upon one another to help you understand the *who*, *what*, *where*, *when*, *why*, and *how* of successful organizational cybersecurity. With that said, readers can also flip through this book to specific sections to find useful discussions on topics of interest for an organization and its cyberdefense program.

Chapters

This book contains the following chapters:

- **Chapter 1: The Digital Organization** describes various aspects of the modern digital organization, including how the rise of IT transformed how modern organizations operate and why they need to be secured.
- **Chapter 2: Ever-Present Cyber Threats** explores cyber threats and the people behind those threats. It examines the challenges of identifying attackers (the attribution problem) and why enforcement action against attackers is so difficult (the prosecution problem).
- **Chapter 3: Cyber Risk Management** details the risk management process in terms of assets, vulnerabilities, threats, risks, risk severity, risk treatments, and countermeasures.
- **Chapter 4: Cyberdefense Concepts** describes security controls, audits, assessments, and cybersecurity capabilities. It defines what a control is and how controls can be used to protect IT systems such as networks or applications.
- **Chapter 5: Cybersecurity Drivers** describes how laws, regulations, cyberdefense standards, contractual obligations, liabilities, and insurance will drive the requirements for an organization's cybersecurity program.
- **Chapter 6: Cyber Program Management** considers how the organization can operate its cyber program within the larger organization, and in the context of other, competing, business priorities.
- **Chapter 7: Cybersecurity Capabilities** details the concepts of cybersecurity capabilities and cybersecurity frameworks. It describes how security professionals can employ the capabilities delivered by available security technologies to deliver cyber controls that mitigate cyber threats and risk.
  Chapter 8: Cybersecurity Operations describes some of the processes that should be implemented by the organization's cyber program to operate its cybersecurity capabilities and cyber controls so they are effective.
- **Chapter 9: Cyber Awareness** explains how our daily actions can affect our security posture at work, at home, and on travel.
- **Chapter 10: Organization Cyber Awareness** considers how the interwoven activities of personnel, customers, partners, service providers, vendors, and guests affect an organization's security posture.

- **Chapter 11: Cyber Training** explains how cyber awareness and organization cyber awareness can drive an organization cyber training program that is tailored for the needs of all employees, executives, IT staff, security staff, partners, and specialists.
- **Chapter 12: Measuring Cyber Performance** describes how the organization can measure its cybersecurity performance through security metrics, dashboards, reporting, assessments, and audits. It also explores the challenge of knowing when cyberdefense is "good enough."
- **Chapter 13: When Things Go Wrong** considers what happens when the cyberattackers succeed and the organization must move into "crisis mode."
- **Chapter 14: Looking to the Future** examines evolving IT trends such as mobile computing, cloud computing, the internet of things (IoT), blockchain, and cybercurrency. It analyzes how these trends might interact with evolving cyber threats such as supply chain vulnerability and machine speed cyberattacks.

Appendices

This book contains the following appendices:

- **Appendix A: Common Malware Threats** provides descriptions of some common malware approaches, including adware, spyware, and ransomware. It also describes common malware cyberattack methods such as phishing, spear phishing, and industrial espionage.
- **Appendix B: Cyber Awareness and Cyber Training Topics** presents potential cyber awareness and cyber training topics for consideration when developing an organization cyber training program.
- **Appendix C: Example Cyber Policy** provides an example organization cybersecurity policy, organized according to the functional areas used for managing cybersecurity capabilities in this book.
- **Appendix D: Online Cybersecurity Resources** provides a selected compilation of references that can help provide insight into security awareness issues and available cybersecurity training resources.

Glossary

The Glossary provides an explanation of some key cybersecurity terms used in this book, *expressed in plain language* for the professional or casual reader.

Chapter 1
The Digital Organization

Information technology (IT) touches how we stay connected, how we learn and share, and how we conduct business for our work and our family. Thanks to IT, organizations are increasing productivity, reducing costs, streamlining operations, and taking care of people in ways never before possible in history. Some would say the revolution is just getting started.

Don Tapscott famously documented this transition in his 1995 best-selling book *The Digital Economy: Promise and Peril in the Age of Networked Intelligence*.[1] He coined the term "digital economy" to describe the business consequences of this revolution, examining how digitization would affect healthcare, manufacturing, marketing, government, publishing, broadcasting, advertising, human resources, and communication. He also considered some of the looming challenges that would come from this transition in the areas of privacy, regulation, democracy, and society. Figure 1.1 depicts the digitization challenges and digital impacts of his digital economy.

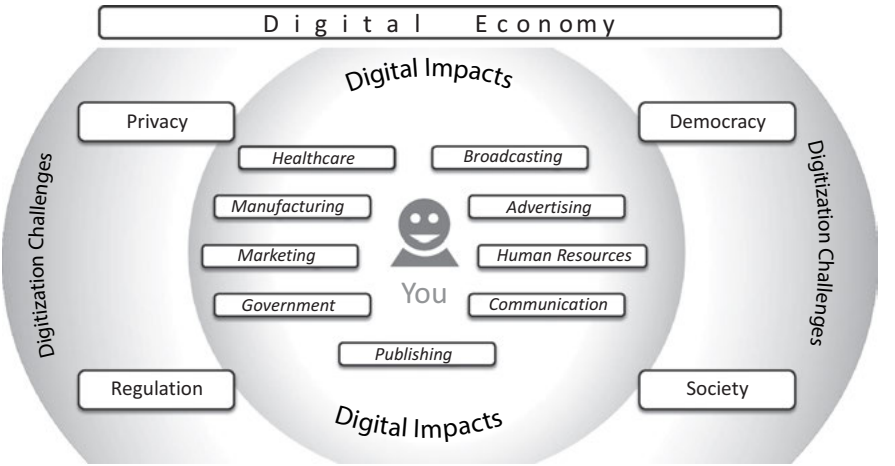


Figure 1.1: Digitization has fundamentally transformed how organizations operate and how employees perform their jobs – along with how organizations implement cyber protections.

1 Tapscott, Don. *The Digital Economy Anniversary Edition: Rethinking Promise and Peril in the Age of Networked Intelligence*, New York: McGraw-Hill, 2015.

https://doi.org/10.1515/9781501506529-001

While Don Tapscott didn't necessarily envision social media businesses like Facebook and Twitter, he certainly understood many of the issues that arose in the decades following the publication of his book.

This chapter describes various aspects of the modern digital organization, including how the rise of IT has transformed everyone's digital life, how modern organizations operate, and need to be secured. It considers how IT has transformed the modern workplace and how that workplace may continue to be transformed in the future. It considers how IT changes the stakes for the modern organization, and the risks that come from those stakes. It considers how people are both a weak link as well as the principal strength in protecting the digital organization. In closing, this chapter will present some historical data related to cyber failures and thoughts on the benefits and threats of computers and ever-present surveillance they can enable.

Everyone's Digital Life

Each of us exists at the center of a "digital life" that includes our work and co-workers, our home and family, and our friends. This connected ecosystem includes computers, tablets, phones, and other resources connecting us to the work and home functions that we use every day. Many of these devices rely upon the internet to work, communicating with computers, servers, and users hundreds or thousands of miles away. Figure 1.2 illustrates this digital ecosystem.[2]

We use these digital ecosystem resources to access work functions including e-mail, calendar, contacts, collaboration tools, and work documents. We also use these resources to access home functions such as e-mail, personal documents, photos, e-commerce, social media, gaming, movies, and music. Sometimes our devices may be dedicated to one function, such as a work computer, but frequently devices and networks may be shared between work and home functions. Examples of this sharing are when we access our work e-mail from a personal phone, or when we send personal e-mail messages from a work computer.

For many of these functions, connectivity to the internet is required. We may get our internet connectivity through office networks, cellular networks,

2 Figure adapted from Donaldson, Scott E., Williams, Chris K. and Siegel, Stanley G. *Understanding Security Issues*, Walter de Gruyter, Inc., 2019.

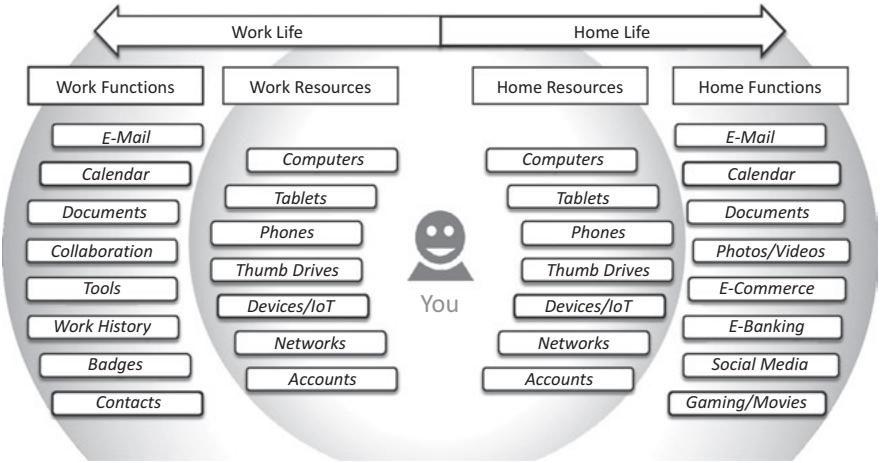


Figure 1.2: Our interconnected digital life requires multiple levels of cyberdefenses for comprehensive protection against modern cyberattacks.

cable modems, satellite services, public Wi-Fi, or other methods. We often use digital identities such as a username and password, or multifactor methods to identify ourselves and prove who we are. Billions of dollars in commerce are conducted each year using online services and online identities, including online banking, e-commerce, healthcare, and collaboration.

Cyberdefenses protecting our digital life must include multiple levels of defense to provide comprehensive protection. These protections must extend to our devices, our networks, our applications, our accounts, and the external partners we trust for our online activities. These protections must be comprehensive, while also unobtrusive, so that we can conduct our online business while also staying protected. People involved in these protections often remain the "weakest link" in the chain of cyberdefense security. Everyone must know how implemented protections work and how to use them so that their online activities can be safe and protected.

IT and the Modern Workplace

Few jobs anywhere have been untouched by IT over the past three decades. For many careers, the disruption has been dramatic and almost continuous since the explosion of personal computing back in the 1980s and the rise of the internet in the 1990s. Digitization has fundamentally changed operational processes

and workflows, fundamentally changing how organizations operate and the work their employees need to perform. McKinsey Global Institute[3] has used the term "digital transformation" to describe these concepts, estimating that most organizations are, even today, operating at a fraction of their "digital potential."

But what is a digital organization? The effects digitization can have on organizations stem from how network-connected digital data differs from the papers and analog recordings that preceded it. These changes can be summed up as follows.

Instant Data Replication

Once data is captured in a digital form and placed onto a network like the internet, it can be made instantly available wherever it is needed, for whomever needs it. It is no longer necessary for data to be manually duplicated (*carbon forms, anyone?*), nor is it necessary for it to be passed among different teams or departments by hand. Similarly, this replication means that large, geographically diverse teams, can have shared situational awareness without having to spend time synchronizing their status.

Real-Time Data Processing

Just as instant data replication means that everyone can have a shared picture of reality, IT permits the data surrounding that shared picture to be analyzed and processed in real time. It is no longer necessary to wait for nightly reports or monthly analysis – IT systems can re-calculate their results in real time, as the inputs change and evolve. And highly powerful computers can perform sophisticated data analytics, in near-real time.

Automated Workflow

Once data is digitized, the workflow around that data and the decisions that must be made regarding it can be automated. With automation, the computer and the network, rather than humans, will enforce the workflow process, reducing errors and dramatically reducing workloads. This automation, in turn,

3 *McKinsey Global Institute* is the business and economics research arm of McKinsey & Company, covering topics such as economic growth, capital markets, technology trends, and urbanization.

frees up the people to focus on the exception cases and situations where judgment is required, rather than just the processes.

Digital Service Delivery

Once the previous three capabilities (i.e., Instant Data Replication, Real-Time Data Processing, and Automated Workflow) are in place, entire services can be delivered electronically with no human intervention whatsoever. These services can include presenting options, taking orders, processing payments, and delivering the resulting services or products. As Amazon has shown with their robot warehouses, even picking, packing, and shipping can be done almost entirely by machine.

Dynamic Social Networking

Employees are no longer limited to the information provided to them by the organizational hierarchy, or the notes they find in the company newsletter. Collaboration and networking tools enable employees, partners, and customers to dynamically share information about what they are doing, where they are struggling, and what help they need. These tools enable people to dynamically self-organize to understand, analyze, and solve problems, multiple times per day.

Advanced Digital Capabilities

Emerging advanced digital capabilities include analytics, machine learning, voice recognition, and machine vision. These capabilities may enable entirely new business functions and opportunities, as we have seen with capabilities like Amazon's Alexa and Tesla's self-driving cars.

Digital Transformation

Thanks to digitization, we now have real-time stock trading at the National Association of Security Dealers (NASDAQ), vendor marketplaces like eBay and Amazon, and ride-sharing services like Lyft and Uber. Digitization has disrupted entire industries, including advertising, communication, transportation, and photography (*remember Kodak?*). These changes have in turn dramatically affected how people do their jobs. Paper processes have given way to e-mail

and online collaboration, file cabinets have given way to data warehouses, and clerks and typists have been replaced with customer service representatives and scanning services. Entire organizations have gone paperless – like the United Services Automobile Association (USAA) did in the 1990s – to leverage the benefits of digitization across their businesses and business functions.

Today, digitization coupled with cloud services has led to the rise of the "fully digital, fully virtual" business. A business using only digital technology no longer needs offices, files, on-premise business systems, or warehouses. Employees scattered around the world can come together using internet collaboration tools, develop products, deliver services, and troubleshoot problems without ever meeting face-to-face. Back-end business functions like payroll, collaboration, communication, sales, and customer service can be delivered over the network, along with storage, archiving, and analysis. By fully leveraging digitization, a business can be freed of many of the old constraints on facility, geography, labor force, and community.

What's at Stake?

John Gall, in his treatise *The Systems Bible*,[4] noted that with complex systems, "the real world is what is reported to the system" and "a system is no better than its sensory organs." *What happens when the entire organization is digital, along with all of its people, connections, collaborations, statuses, and products?* In short, everything becomes vulnerable to digital abstraction, digital distortion, and digital attack.

Digital vulnerability can include corruption, compromise, or deletion of critical data, status, connections, or processes within the digital organization. Depending on the organization, this damage can range from being a minor inconvenience (for the largely non-digital organization) to being an existential threat (for the entirely digital organization). These vulnerabilities translate into organization risks that must be accounted for and considered at an organizational level.

When an organization digitizes, critical information for the organization is converted to digital form and generated, stored, processed, and acted upon digitally. Figure 1.3 depicts examples of such digital information. Critical digital information can include any or all of the following:

4 Gall, John. *The Systems Bible: The Beginner's Guide to Systems Large and Small*, Minnesota: General Systemantics Press, 3rd Edition, 2002.

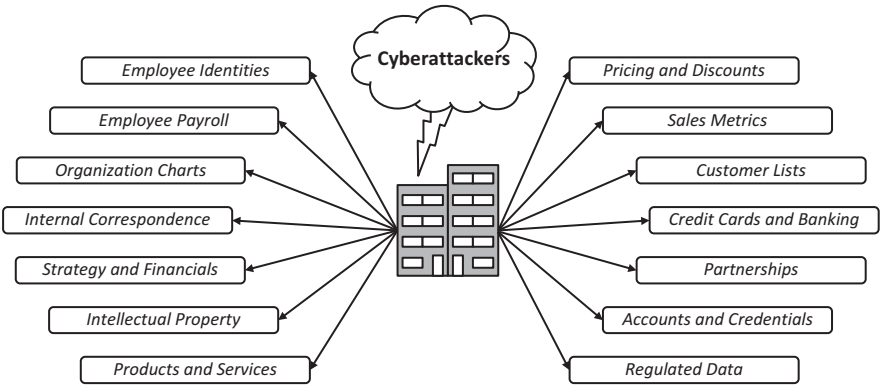


Figure 1.3: Digitization of critical information for the organization introduces cyber risks that must be considered and mitigated.

- **Employee Identities.** Who employees are, along with their personal information about where they live, where they work, e-mail addresses, and online identities.
- **Employee Payroll.** How much money employees make, along with their bank accounts where that money is deposited.
- **Organization Charts.** The structure of the organization, including department structures and reporting relationships.
- **Internal Correspondence.** Internal communications on potentially proprietary and sensitive topics, as well as commentary and opinions that may be embarrassing if publicly released or taken out of context.
- **Strategy and Financials.** Organizational strategic plans and unreleased financial data (particularly for publicly traded organizations).
- **Intellectual Property.** Intellectual property such as inventions, products, services, designs, specifications, and processes that may be proprietary to the organization.
- **Products and Services.** Details on products and services offered by the organization, including upcoming offerings and competitive intelligence.
- **Pricing and Discounts.** Information about pricing for the organization's products and services, including guidance on sales and discount policies.
- **Sales Metrics.** Metrics regarding sales pipelines, revenues, terms, conditions, discounts, refunds, and overall profitability.
- **Customer Lists.** Lists of customers and customer contacts, along with information regarding contact points, meetings, schedules, and follow-up actions.

- **Credit Cards and Banking.** Details about customer and partner financial accounts, including credit cards, bank accounts, billing cycles, account balances, and payment records.
- **Partnerships.** Information about partners and partnerships, including partnership terms and conditions, strategic objectives, shared pipelines, and points of contact.
- **Accounts and Credentials.** Login accounts and credentials for customers, partners, and employees that may be used with organization systems and may be exploited elsewhere due to credential re-use.
- **Regulated Data.** Other data that may be regulated or restricted by local or national governments. This data may be related to identity, privacy, healthcare, finances, or numerous other protected criteria.

Breach, alteration, or destruction of any of this information can result in situations that are awkward, embarrassing, or time-consuming at best. At worst, such damages will be expensive, disruptive, and may be even disastrous to the organization, to say nothing of the careers of its leadership. Digitization, for all of its positive power, introduces new risks to the organization and its business that must be considered and mitigated. These risks include complex computing environments, complicated compliance requirements, and the ever-present lack of sufficient resources to do everything that is required or desired.

The Rise of Cybercrime

Digitization challenges have led to whole new industries of cybercriminal activity. *Why try to rob a bank using guns when the internet enables a cybercriminal to steal using a computer, and from the comfort of the criminal's own home?* With cybercrime (and its cousin, cyber espionage), data is the property, currency, and objective, and such data is often deceptively accessible using the global internet.

In his book *Spam Nation*,[5] Brian Krebs observed that, thanks to weaknesses in the credit card transaction processing system, "cybercrooks [are] hitting one major retail chain after another, laughing all the way to the cash machine." Brett Kingstone, in *The Real War Against America*,[6] wrote that "the cost to the U.S. economy from the continued theft of our technology may eventually reach

5 Krebs, Brian. *Spam Nation: The Inside Story of Organized Cybercrime – From Global Epidemic to Your Front Door*, Illinois: Sourcebooks, Inc., 2014.

6 Kingstone, Brett. *The Real War Against America*, Specialty Publishing, 2005.

more than $250 billion per year." And Brett's cost estimates are from more than a decade ago. More recently, the Center for Strategic and International Studies (CSIS) estimated the 2018 global cost of cybercrime to be $450 billion, with another $150 billion per year lost to cyber espionage. That's real money.

Cybercrimes range from theft of credit card numbers to medical records, bank accounts, user credentials, proprietary technologies, industrial hardware, and military secrets. Many of these thefts are perpetrated by individuals and criminal syndicates, while others are performed by international state-sponsored intelligence agents. Cybercrime is big business, and it is only getting bigger.

Protecting the Organization

Digitization creates entirely new ways for things to go wrong, creating new business risks that must be considered by leadership alongside other security, operational, and organizational risks. *If digitization is so risky, why do it at all?* Simple! Because the advantages of digitization and connectivity – agility, speed, cost reduction, quality, resilience, and new capabilities – are so compelling that organizations simply have no alternative if they are to endure and remain relevant. Digitization *must* be employed, and the organization *must* find a way to do it "safely" by employing appropriate defenses to protect it. Protection can include many things – often categorized as *people, process, and technology factors* – for guarding the digital organization and its data from harm.

Protection of digital systems, networks, and data has become an industry unto itself. Just as one can go to the security aisle of the local home improvement store and find locks, keys, cameras, and alarm systems, the cybersecurity industry has created a dizzying array of technologies and capabilities for protecting today's computers, networks, devices, accounts, and digital data. At an organizational level, cyber protection technologies can approach or even exceed the complexity of the IT systems they are protecting. Protections may include interconnecting digital "walls," "gates," sensors, and response components, all working together under the purview of the organization's cyber defenders. These defensive capabilities generally fall into the following categories.

- ***Preventive:*** Preventive technologies are the most obvious security measures, since they are intended to *prevent* malicious activity from occurring. Endpoint security tools can prevent malware from running on protected computers, e-mail filtering can prevent malicious messages from getting through, and network firewalls can prevent malicious network traffic from entering the organization. Prevention is attractive, since it means harmful things are blocked or prevented from occurring.

- ***Detective:*** However, prevention can seldom provide complete protection. An old joke goes that all malicious computer behavior can be prevented, if you just turn the computer off. Any time people are permitted to do things, there will be scenarios where it is possible for malicious behavior to occur, and prevention may not always be feasible, practical, or economical. In those cases, *detection* can fill the gap by detecting such behavior or its consequences. This detection can then generate an *alert* for later *response* by cybersecurity personnel.
- ***Response:*** Once the organization has the ability to detect certain types of malicious behavior, it then needs cybersecurity tools, operational resources, and trained personnel who can mount a *response* to the detection alert. Responses typically occur when signs of malware, malicious user behavior, or malicious network traffic occur in the organization. Response personnel will then investigate the alert, contain the threat, and remediate the damage that was done.
- ***Recovery:*** When the organization responds to cybersecurity alerts, it may also find that it has to perform *recovery* actions to restore normal operations after the cyberattack. Computers compromised by malware may need to be removed from the network and then cleaned or re-imaged with known, good software. User accounts may have to be locked and their passwords changed. Malicious network traffic may have to be blocked and their sources and destinations identified. Corrupted data may have to be restored from backups or corrected to remove the corruption.

A balanced cyberdefense consists of elements of all four of these categories, working together to prevent, detect, respond to, and recover from a variety of cyberattack scenarios. These scenarios may range from untargeted malware (e.g., viruses, trojan horses, worms, spyware, adware) to nation-state sponsored ransomware attacks. A balanced cyberdefense should be designed to block the most common cyberattacks while also being able to detect and respond to those attacks that slip through the initial defenses. A balanced cyberdefense should also include recovery capabilities that allow the organization to restore its computers, data, IT systems, and applications, should a failure occur. An *all-hazards defense* will include robust cyberdefense capabilities that can help protect and restore IT systems against a wide range of possible hazards, ranging from remote cyberattacks to natural disasters.

The People Factor

People are, simultaneously, both the strongest and the weakest link in any defense. Looking at their weaknesses, humans are fallible, error-prone, and easily distracted. They are also good-intentioned, helpful, and hesitant to disagree. These human characteristics are anathema to operating a disciplined and rigorous defense, particularly one that must resist attack from malicious and professional attackers who are intent on achieving success at any cost.

Ironically, one of the greatest challenges in effective cyberdefense has to do with managing the complexity of the defense itself. In his book *The Mythical Man-Month*,[7] Frederick P. Brooks Jr. points out that complex systems have an irreducible number of errors – for every glitch one fixes, the fix introduces other bugs or glitches. *What does Brooks' observation have to do with cyberdefense?* Everything!

No complex cyberdefense system can be expected to perform perfectly, all the time – especially when the system is created, installed, maintained, and operated by people.

Cyberdefenses must be designed around the assumption that failures will occur. E-mail will bypass screeners; malware will evade anti-virus software; network connections will be allowed to traverse the network; and cyberdefenders will miss alerts. Things are going to go wrong, and people are going to make mistakes that cause the first-line cyberdefense to fail.

What happens after the first line of cyberdefense fails? Is there a second line of cyberdefense? How about a third line of cyberdefense? The most effective organizations will have answers to these questions, so that a single failure or a single mistake is the beginning of the defense, not the end.

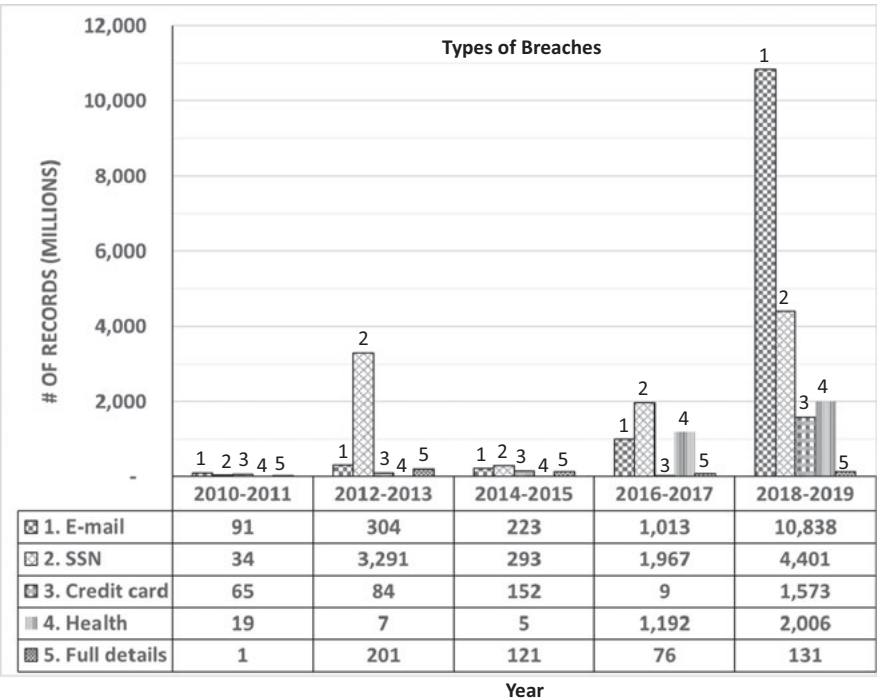
Real-World Cyber Failures

In practice, cyberdefense seldom works out so elegantly that layers of defenses seamlessly interact with each other and their human masters, blocking cyberattackers at every turn while keeping employees, partners, and customers safe every day. While the reality is that every day, millions of cyberattacks are in fact thwarted successfully, it only takes a couple of failures to make headlines and affect millions of people. In a world where a person's entire genetic code

---

7 Brooks, F.P. *The Mythical Man-Month: Essays on Software Engineering/Anniversary Edition*, Boston: Addison-Wesley, 1995.

can fit onto a portable drive, cyberattackers can easily obtain and extract records for millions or even billions of individuals in a single cyberattack. These records may be as simple as an e-mail address, as secret as a password, or as comprehensive as a complete medical or financial history. Figure 1.4[8] is a ten-year summary of 288 breaches, where each breach consisted of more than 30,000 records per breach. Combined, these breaches exposed over 28 *billion* records.



	2010-2011	2012-2013	2014-2015	2016-2017	2018-2019
1. E-mail	91	304	223	1,013	10,838
2. SSN	34	3,291	293	1,967	4,401
3. Credit card	65	84	152	9	1,573
4. Health	19	7	5	1,192	2,006
5. Full details	1	201	121	76	131

Figure 1.4: Cyberattacks have exposed over 28 billion records containing e-mail information, social security numbers, credit card information, health, and personal information.

As shown in the lower left of Figure 1.4, the *breaches* are broken into the following five categories of breach:

1. E-mail and online information
2. Social Security Number (SSN) and personal details

8 Data Source: https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/.

3. Credit card information
4. Health and personal records
5. Full [record] details

Each cell counts millions of breached records, by two consecutive calendar years. Some of these breaches involved credit card numbers or banking information and were most likely perpetuated by cybercriminals looking to use that information for fraudulent transactions. Some breaches involved usernames and passwords and may have been performed by hackers looking to use those passwords to access other, more profitable accounts (since people often reuse passwords for multiple online accounts). Some breaches involved health care information, which tends to be a treasure trove of highly personal data, as well as financial details. Finally, some breaches involved potentially embarrassing personal information; this information might be used to blackmail individuals to get their cooperation.

Most breaches involved *social security numbers* and *e-mail* – approximately 22.5 billion records.

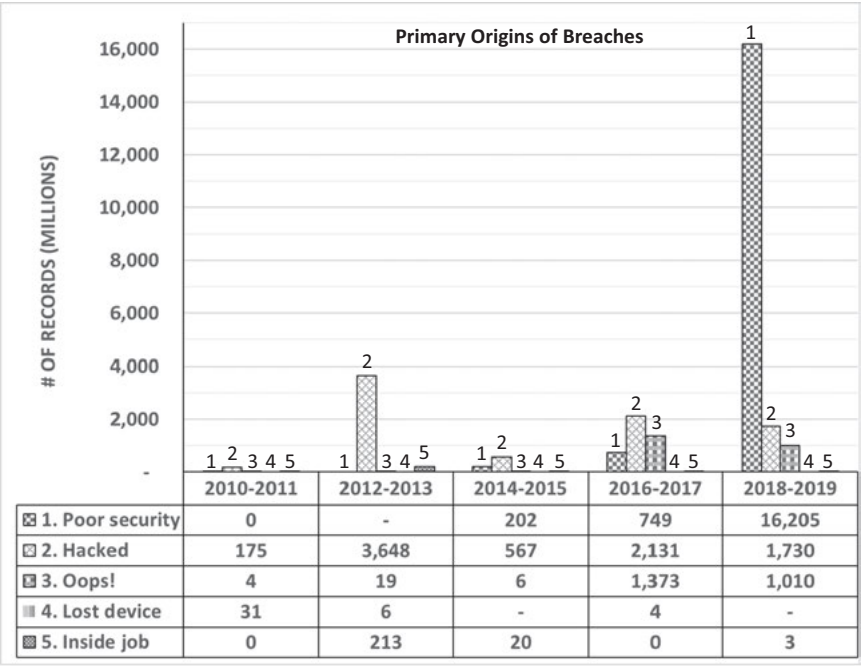
Figure 1.5[9] shows further analysis of the data in Figure 1.4, considering the *primary origins* of the breaches that occurred.

As shown in the lower left of Figure 1.5, the breaches are broken into the following five categories of primary origins:

1. Poor security
2. Hacked (accounts/devices being hacked)
3. Oops! (people making mistakes)
4. Lost device (people losing devices)
5. Inside job (people inside organization conducting malicious attacks)

Each cell counts millions of breached records, by two consecutive calendar years. The totals may not match Figure 1.4 perfectly, due to rounding and other factors. As can be seen in the table, these breaches range from thousands of records to millions of records to over a billion records for the largest breaches. Organizations under attack include those with less than a few dozen people to thousands of people to international organizations with tens of thousands of people. Market sectors attacked include energy, industrials, consumers, health

9 Data Source: https://informationisbeautiful.net/visualizations/worlds-biggest-data-breacheshacks/.



	2010-2011	2012-2013	2014-2015	2016-2017	2018-2019
1. Poor security	0	-	202	749	16,205
2. Hacked	175	3,648	567	2,131	1,730
3. Oops!	4	19	6	1,373	1,010
4. Lost device	31	6	-	4	-
5. Inside job	0	213	20	0	3

Figure 1.5: Cyberattacks are due, in part, to poor security, accounts being hacked, people making mistakes, people losing devices, and people inside the organization conducting malicious attacks.

care, financials, information, telecom services, the government, utilities, education, and others.

Most breaches involved *hacked accounts* and *poor security* – approximately 25.4 billion records.

In general, the number of exposed records continues to trend upward, even with an increased emphasis on implementing sophisticated cyberdefenses and increasing societal cyber awareness. As things get more complicated, the likelihood of exposing records increases, despite all the attention.

What Does It All Mean?

As Bruce Schneier pointed out in his book *Data and Goliath*,[10] "the benefits of computers knowing what we're doing have been life-transforming . . . [but] . . . the threats of surveillance are real, and we're not talking about them enough." What happens when:

- *Apple or Google is tracking everywhere you go, every day, thanks to your mobile phone reporting its location to them?*
- *Yahoo is analyzing every e-mail you send or receive for its advertising potential?*
- *Facebook is analyzing your social network to understand which of your friends is most influential on your behavior, and then is suggesting to its advertisers that they reach out to your friends to try to turn you into a buyer for their products?*
- *These surveillance capabilities are applied to your friendships, your preferences, or your politics?*
- *This so-called "private" data ends up in the hands of criminals, unfriendly states, or is simply published on the open internet, for everyone to see?*

These possibilities are endless, and frightening.

10 Schneier, B. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, New York: W.W. Norton & Company, Inc., 2015.

Chapter 2
Ever-Present Cyber Threats

Once an organization becomes digital, it is transformed both for better and for worse. For better, because it is more agile, more responsive, and more capable than it ever was before. For worse, because those same transformative digital capabilities introduce a new vulnerability . . . to cyberattack. With this new vulnerability comes new questions, new concerns, and new risks. *What threats do cyberattacks pose to digital organizations? Who are the hackers carrying out these cyberattacks? What do these hackers want? How are they making money? How do they accomplish their goals? What do their real-world cyberattacks look like? How do organizations' cyberdefenses counter their attacks?* These questions, and their answers, help us to better characterize the hackers we are up against, how they operate, and what we can do about them.

This chapter explores ever-present cyber threats and the people behind those threats. It considers the different types of hackers, their motivations, and objectives. It describes the objectives hackers may have against their victims and the methods they may use to accomplish their objectives. It examines the challenge of identifying cyberattackers (the attribution problem), and why enforcement action against hackers is so difficult (the prosecution problem). It illustrates what real-world cyberattacks look like when perpetrated by real-world hackers against real-world victims to accomplish real-world objectives. The chapter then examines how cyberdefenses may seek to disrupt, detect, delay, and defeat these cyberattacks before they can be successful. By thoroughly understanding these threats, an organization can focus its attention on the defensive techniques that may be most helpful or promising.

Who Are the Hackers?

Hollywood and television have perpetuated a stereotype of the "lone wolf" hacker working out of a basement apartment. Anyone who has gone to the DEF CON conference – one of the world's largest hacker conventions – will tell you that there are plenty of people who really do look like this Hollywood stereotype.[1] However, there are many others who do not reflect the stereotype and are

1 McKeay, Martin. "Researching the Psychology of Hackers," Security Intelligence, December 2, 2015 (https://securityintelligence.com/researching-the-psychology-of-hackers/).

https://doi.org/10.1515/9781501506529-002

working for professional organizations, governments, or organized criminal groups. The reality is that hacking has become big business. Stereotypes aside, most hackers fall into one of the following categories.

Casual Hackers

A casual hacker is someone who hacks simply for the fun of seeing what can be accomplished. *Can I "outsmart" the defenses of an operating system, application, or that new connected device? Can I find vulnerabilities in the systems used by individuals, corporations, or governments? Can I create a piece of malware all by myself, and can it propagate in the wild? Can I use that new hacking toolkit I found online, and do its tools work as advertised?* What distinguishes casual hackers is that they are doing it for the "joy" of figuring things out or proving their own abilities.

Showboat Hackers

A showboat hacker is someone who has a know-it-all attitude and is seeking to show off their talents, abilities, and superiority. Showboat hackers often have a bone to pick with someone or some organization. They may want to get even with someone; damage computers, smart devices, or data because they can; or simply grandstand by embarrassing their victims. Showboat hackers can make excellent candidates for those who make hacking a profitable business. Hacker conventions tend to be good recruiting venues for showboat hackers, who seek to show off their skills and garner attention.

Hacktivists

As popularized by the USA Network TV show "Mr. Robot," the hacktivist probably lies closest to the Hollywood hacker stereotype. The show's central character is a software programmer who is a cybersecurity engineer at work during the day and a "vigilante" hacker in his off-hours. While casual hackers hack for the sheer pleasure of figuring things out and showboat hackers hack to get even, hacktivists tend to have more focused objectives.

Hacktivists want to make a point, prove someone wrong, or embarrass an individual or organization. They are hacking to support some ideological objective; not necessarily just for personal or financial gain. "Anonymous" is probably

the most famous online hacktivist group, conducting cyberattacks against governments, corporations, and organizations. Some people would argue that Edward Snowden, who leaked highly classified U.S. National Security Agency (NSA) information, and Wikileaks, which publishes leaks of US classified information, are also conducting "hacktivist" activities.

Cybercriminals

If hacktivists have the ability to get big publicity, cybercriminals have the ability to make big money:

"New criminality platforms and a booming cybercrime economy have resulted in $1.5 trillion in **illicit profits** [emphasis added] being acquired, laundered, spent and reinvested by cybercriminals [in 2018]

$860 billion – Illicit/illegal online markets
$500 billion – Theft of trade secrets/IP [Intellectual Property]
$160 billion – Data trading
$1.6 billion – Crimeware-as-a-Service
$1 billion – Ransomware"

–Dr. Michael McGuire[2]
Senior Lecturer in Criminology
University of Surrey in England

What activities are considered cybercrime? The answer is not as straightforward as some people may think. Hackers are pursuing their own priorities and serving causes they believe are in their self-interest or their employers' interests. Even anarchists seeking to undermine the world's safety and security have a point to make, if others choose to listen.

The U.S. Department of Justice, Bureau of Justice Statistics characterizes cybercrime as follows:[3]

- Cyberattacks against computers involving computer viruses (e.g., worms, Trojan horses), denial of service attacks, and electronic vandalism or sabotage
- Cyber theft using computers to steal money or other things of value (e.g., intellectual property, personal or financial data, fraud, embezzlement)

---

2 McGuire, Michael. "Hyper-Connected Web of Profit Emerges, As Global Cybercriminal Revenues Hit $1.5 Trillion Annually," GLOBE NEWSWIRE, April 20, 2018.

3 Material adapted from U.S. Department of Justice, Bureau of Justice Statistics website: https://www.bjs.gov/.

– Other computer security incidents (e.g., spyware, adware, hacking, phishing, spoofing, pinging, port scanning, and theft of other information)

One definition of cybercrime is: any illegal activity involving the internet, information technology (IT) (e.g., computers, networks, telecommunications, databases, and software), information systems (e.g., office automation systems, management information systems, decision support systems), or people (individuals, employees, executives).

Cybercrime may be perpetuated by individual criminals, but is often performed by professional groups pooling the resources of hackers, criminal minds, stolen identities, illicit bank accounts, and even telemarketers and customer service. Criminal groups may employ hacking as only one of many tools to achieve their objectives of fraud, theft, blackmail, or ransom.

The key to cybercriminal behavior is a financial objective. While cybercriminals may have an indirect objective – such as stealing data, identities, or locking out systems – most often, cybercriminals' ultimate goal is to monetize their objective. They may accomplish this by selling it to others, emptying bank accounts, or getting the victims to pay cash for explicit relief or perceived peace of mind.

Nation-State Attackers

While cybercriminals almost universally have a financial goal as their ultimate objective, nation-state attackers may attack for more abstract purposes, based on the needs and goals of their country's government. Sometimes, nation-state goals may be financial. For example, North Korea has been accused of using hacking to bypass sanctions and obtain international currency. More often, nation-state goals are political, such as getting information about other countries' people, businesses, technologies, or governments. Nation-state goals may also be destructive, such as Russian hacking against Chechnya and Ukraine during 2016 and 2017. Russian hacking included attacks on Ukraine defense, financial, and power-generation infrastructures. Nation-state hacking has been cited in the disruption of Saudi Aramco's oil exploration in 2012, Sony Pictures' entertainment business in 2014, and Maersk's global shipping in 2017.

"White Hat" Hackers

White hat hackers, sometimes called "ethical hackers," perform authorized hacking for the "good guys." This is in contrast to "black hat" hackers who perform

hacking that is unauthorized and criminal in nature. White hat hackers use the same hacking tools and techniques as the black hats, but to legitimately assist organizations with improving their cybersecurity. What distinguishes white hat hackers from other types of hackers is their adherence to codes of ethics and rules of behavior. Their mission is to perform hacking so it is in the best interests of the affected organization. White hat hackers who penetrate defenses do so with the permission of the targeted organization.

White hat hackers may perform penetration testing, participate in "bug bounty programs,"[4] perform social engineering, or do vulnerability research. White hat hackers may be employed by cybersecurity solution providers, academic institutions, or the target organizations themselves. Their goal is usually to identify vulnerabilities, educate the organization about the vulnerabilities, and make recommendations about how the organization can improve its defenses. White hat hackers who find cybersecurity weaknesses and vulnerabilities bring them to the attention of the targeted organization rather than exploiting the vulnerabilities for profit. White hat hackers who create malware publish it, along with appropriate detections, defenses, and remediations to protect against it.

Know Your Attacker

Of course, these hacker category distinctions are not always clear-cut. Just as the protagonist in "Mr. Robot" gets recruited into professional, malicious hacking, today's casual hacker may become tomorrow's professional. At the international level, it is not uncommon for nation-states to employ cybercriminal groups to accomplish their political goals while simultaneously turning a blind eye to the groups' other, less-savory activities. Kevin Mitnick, who was the FBI's "Most Wanted Hacker" in the mid-1990s, went legitimate and became a famous and popular white hat hacker (after publishing a bestselling memoir, of course). Knowing who one is up against can be very helpful when considering what types of defenses are appropriate, and to what level those defenses should be performed.

4 An arrangement where individuals can receive compensation for identifying and reporting "software bugs" (i.e., computer program errors) to organizations (e.g., Netflix, Starbucks, PayPal, Twitter).

The Cybercrime "Attribution Problem"

It would be easier to identify hackers if they left fingerprints, getaway cars, or other telltale signs when they strike. But the fact is that in the cyber world, everything is fungible and it is impossible to be sure whether evidence is legitimate or simply left behind to obfuscate the truth. Obtaining and preserving evidence that would stand up in court is difficult. This challenge is sometimes referred to as the "attribution problem."

Bruce Schneier, who is an internationally renowned security expert, summed the attribution problem up very well in 2014 when he stated that the hack against Sony Pictures "may have been performed by the full might of the North Korean military, or it may have been performed by two guys in a garage – we're just not sure." Because the internet instantly connects computers around the world, and software written anywhere in the world can run anywhere else in the world, it is hard to know exactly where the people are behind any given computer activity.

With these limitations in mind, there are techniques cyberdefenders use to attempt to identify who attackers are and where they come from. Some of these techniques work better than others, and none of them is 100% effective or reliable. When cybersecurity experts state that an attack came from a certain attacker group or organization, they are usually coming to this conclusion based on one or more attributes of the attack that they identified in their investigation. Some of these attributes are described as follows.

Network Addresses

Certain groups have network infrastructure around the world, including proxies, servers, command-and-control computers, and botnets under their control. This infrastructure can then be recognized by its network internet protocol (IP) addresses or domain name system (DNS) names.

Network Protocols

Just as certain groups may have distinctive infrastructure that they use, groups may also be recognizable by the network traffic of their malware or of their command and control channels. This traffic may contain distinct patterns, signatures, or sequences that are unique and distinct. Such traffic may be recognizable even when the malware itself has been changed or when a different internet infrastructure is being used.

Software Code

Certain groups use certain software, or modules within larger software systems. Since there is nothing stopping other groups from also using the same software, software code is one of the weaker attribution methods. However, the use of specific software may be an indicator of the hackers or groups involved, particularly when corroborated by other indicators.

Software Behavior

Similarly, certain groups may have distinctive *modus operandi* among their malware or command sequences. The same behavior at multiple target organizations may indicate a single group is driving all of the attacks, even if other aspects of the attacks are different from victim to victim.

Software Language

Malicious software may contain indicators – such as programming language properties, comments, or error messages – written in specific languages that may point to the country of origin. While this factor may not indicate the specific group involved, just knowing the country of origin may be helpful. In addition, coding style might help identify hackers or groups, although it is not a fingerprint.

Exploits

The use of particular exploits can be distinctive to attack groups, particularly when those exploits are "zero-day" exploits[5] that were unknown before their use in a particular attack. Because zero-day attacks target vulnerabilities that were previously unknown, they can be particularly effective, though their use is uncommon outside of nation-state attacks. What is more common is for

5 A zero-day exploit is a cyberattack that targets a vulnerability not publicly known or for which a patch is not yet available. Zero-day exploits are valuable to attackers because they can be difficult or impossible to block. However, the use of a zero-day exploit can reveal the underlying vulnerability and give defenders the opportunity to mitigate it.

attackers to target vulnerabilities that are known, but simply have not been patched yet. This is why patching and vulnerability management is so critical for internet-connected organizations.

Attack Campaigns

Specific groups tend to launch attacks in campaigns, using the same or similar malware, network infrastructure, tools, techniques, and procedures at multiple victim targets over the course of a brief period of time. Attackers use such campaigns because they know the defense community will recognize their attack and attempt to protect itself. So it pays to use new attack methods as widely as possible before effective defenses can be mounted.

Attack Commonalities

Similarly, there may be other attributes like bitcoin accounts, e-mail addresses, websites, or malware patterns that enable an unknown attack to be linked with other, previously known attacks. Using such attributes, defenders can frequently link together multiple attacks into "campaigns" most likely being conducted by a single attacker group. However, even though the campaign may be recognized, who is "behind the scenes" making the attacks happen may still be left unknown.

Obfuscation

Unfortunately, just as defenders have tools for trying to trace down who the attackers are, attackers have just as many tools for hiding their origins and identities. Attackers can hide their identities by obfuscating their code, encrypting their communications, and hiding their command and control nodes behind multiple layers of proxies. These attacker tools make it harder for defenders to know who they are up against. For example, cyberattacks against a university's servers may be originated from compromised personal computers within that same university's network, making identifying the source and attributing the attackers more difficult. Similarly, attacks against a corporation may be originated from that corporation's competitor, just to cause headaches for both organizations and allow the attackers to slip away while the companies are potentially bickering with each other.

The Cybercrime "Prosecution Problem"

Many governments – including the United States, United Kingdom, European Union, Russia, China, and India – have enacted national regulations governing cybersecurity and outlawing various forms of cybercrime. While enforcement of these laws may be uneven across different countries (and even more so when crossing international boundaries), the fact is that most governments take cybersecurity seriously, especially when it causes harm to their citizens and constituents. Lawmakers and government leaders generally understand the consequences of cyber breaches to people's privacy, money, health, identity, and relationships. The lawmakers and government leaders try to pass laws and create regulations intended to help reduce the risk of those cyber breaches – even if it may not always feel like the laws and regulations are actually working.

Even with laws supporting them, prosecutors may not have a legal ability to arrest people who live in affected jurisdictions. Nonetheless, computer criminals have been caught and convicted of cybercrimes in Australia, Canada, England, Russia, South Africa, United States, and Ukraine, to name a few countries. Cyber prosecution has included fraud (e.g., identity, wire, bank), unauthorized access to computers, stealing credit card numbers, trespassing onto computer networks, hacking cell phone accounts, money laundering, unauthorized access of business information systems, and writing and distributing computer viruses. Cyber punishment has included financial restitution, fines, and prison time.

Unfortunately, the reality is "the total cost of cybercrime is expected to exceed $2 trillion this year [2020] . . . a four-fold increase when compared to the estimated cost of cybercrime in 2015."[6] Cybercriminals may believe their chances of getting caught are low, so why not take the risk and steal a million credit card numbers that can then be sold on the dark web? The benefits of cybercrime frequently outweigh the risks of getting caught. Robbing an individual *face-to-face* is a high-risk venture, when compared to robbing thousands or millions of people *virtually*.

Cybercrime is a big-money *virtual* business with relatively low risk when compared to traditional *face-to-face* crime. Until the risk/benefit changes, cybercrime will continue to get worse.

6 Mardisalu, Rob. "14 Most Alarming Cyber Security Statistics in 2020," January 6, 2020: https://thebestvpn.com/cyber-security-statistics-2020/.

What Do the Hackers Want?

What do these hackers want to accomplish? Put simply, hackers want to gain access to computers and devices belonging to an organization, and then use that access to get to the organization's networks, computers, applications, sensitive data, and operational processes. These cyberattacker objectives can be characterized by the words *confidentiality, integrity, and availability* (CIA) and are often visualized as a triad, as shown in Figure 2.1.[7]

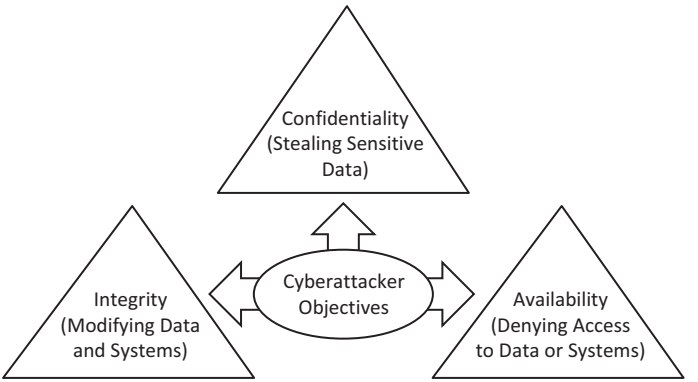


Figure 2.1: Cyberattackers target confidentiality, integrity, and availability.

This CIA triad is important because it can be used to abstractly define almost every type of cyberattack and characterize the cyberdefenses used to counter those attacks. For example, if a cyberattacker seeks to violate the *confidentiality* of sensitive data, then the corresponding cyberdefense seeks to *protect* that confidentiality. Similarly, cyberdefense measures can also protect the *integrity* and *availability* of organizational data, computers, networks, and operational processes. At the next level of detail, the cyberattacker objectives can be characterized as follows.

Confidentiality: Stealing Sensitive Data

This cyberattacker objective involves gaining access to sensitive data intended to be kept private or confidential. Such data might include credit card or bank

7 Figure adapted from Donaldson, Scott E., Williams, Chris K., and Siegel, Stanley G., *Understanding Security Issues*. Walter de Gruyter Inc., 2019.

account numbers, personal information such as e-mail addresses, home addresses, usernames, passwords, or cryptographic keys. Confidential data can also include an organization's proprietary information that may include intellectual property, trade secrets, private correspondence, business strategies, customer lists, product designs, or unreleased financial reports. Attackers bent on a confidentiality attack seek to defeat the protections around such data to obtain access to it. Once attackers obtain access to the data, they may seek to copy or download the data from the victim's computer systems.

Integrity: Modifying Data and Systems

This cyberattacker objective involves changing data or processes on computer systems. Attackers may falsify data to throw the victim organization into disarray through confusing or contradictory guidance, or may steal money by changing account numbers or generating fraudulent financial transactions. Attackers who gain access to account secrets like usernames and passwords or cryptographic keys may change them, locking out the authorized users. Integrity attacks, when applied to trusted communication channels like official Twitter accounts, corporate web pages, or official internal processes, can cause great confusion and embarrassment for victim organizations.

Availability: Denying Access to Data or Systems

This cyberattacker objective involves destroying, disabling, or encrypting data or systems, so they are unavailable to the intended users or audience. These attacks can be particularly disruptive for target organizations, depending on the magnitude of the destruction and the victim's ability to contain and recover from the attack. Two popular forms of availability attacks are *distributed denial of service (DDoS)* and *ransomware*. DDoS attacks disable internet-connected computers by overloading them with massive quantities of network traffic. Ransomware attacks disable computers by encrypting their data and then charging a ransom payment to get the decryption key. Other availability attacks may delete data or even permanently damage computer equipment like motherboards or hard drives. Availability attacks test an organization's ability to detect, contain, remediate, and recover from the attack, while reducing the operational impact of the impaired systems.

What the Hackers Want

For casual hackers, showboat hackers, hacktivists, and nation-state attackers, the satisfaction of an attack successfully executed may be the primary compensation, but for professional cybercriminals the goal is most often financial. For professional attackers, once the primary attack objective – confidentiality, integrity or availability – is satisfied, the secondary objective is usually to monetize that accomplishment. Professional attackers may monetize their attacks by selling confidential data on black markets, selling access to compromised accounts and networks, creating fraudulent transactions to drain victim bank accounts, or blackmailing their victims into paying for access to their data or to keep compromised data secret. This behavior is helpful to law enforcement, who may be able to "follow the money" to find and convict the actual attackers even if their online identity cannot be ascertained for certain.

How Do Hackers Accomplish Their Goals?

To accomplish their goals, hackers have a dizzying array of tools at their disposal. Open-source exploit toolkits include testing platforms like MetaSploit, network scanners like Nmap, vulnerability scanners like Nessus, and operating system platforms like Kali Linux. Many of these tools are "open source," which means the attackers can read the source code to incorporate specific capabilities into their malware software modules. In addition, numerous books have been written on hacking techniques and exploit methods. Malicious hackers use these tools, techniques, and procedures to do harm, while white hat hackers and penetration testers use many of the same tactics to help organizations improve their security. Network-connected computer systems are notoriously complex, with many vulnerabilities inherent in the complexity. Making systems secure and then keeping them secure over time takes diligent, meticulous effort by skilled practitioners. As shown in Figure 2.2, this section describes some of the tools and techniques used by cyberattackers to accomplish their goals.

Malware

Malware[8] is software explicitly written for nefarious purposes. Such software may steal user credentials or credit card numbers, provide backdoor access to computer

8 *Malware* is short for *mali*cious soft*ware*.

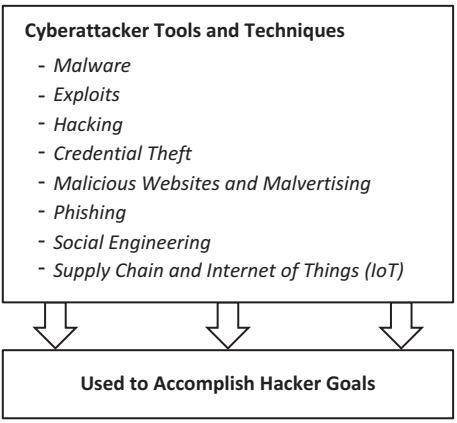


Figure 2.2: Cyberattackers use a number of tools and techniques to penetrate organizations' cyberdefenses.

systems or mobile devices, or permit the bypassing of security features like firewalls, detection sensors, or anti-virus software. There are literally millions of strains of malware. While anti-virus software is good at recognizing malware that is known, new versions and variants of malware are released continuously.

Exploits

These are pieces of software code that enable accessing and installing malware onto computer systems without the permission of the system operators. Exploits can take advantage of a vulnerability by forcing a targeted computer or device to run additional code provided by the attacker. The additional code may then be used to install malware, open up access, or install attacker credentials onto the system so the attackers can maintain their access.

Hacking

The act of obtaining unauthorized access to computer systems, usually by exploiting vulnerabilities in computer system security. "Hacking" refers to actions performed by the attacker to gain access to victim computer systems, maintain that access, move laterally, escalate privileges, access data, or exfiltrate compromised information out of the target computing environment. Attackers may hack internet-facing servers to gain access to the servers and the networks

behind them, or they may hack user endpoints to gain entry to organization networks or steal user credentials. Many attacks require multiple steps of hacking, as the attackers navigate victims' networks to find the systems and data that are of interest.

Credential Theft

This illicit activity involves stealing user credentials – most often, usernames and passwords – to gain access to victim computer systems and networks. This access can be particularly useful for cloud-based services, where account credentials may be the only line of defense. Frequently, attackers seek to gain access to *privileged accounts* used for systems administration. These accounts may have access to large numbers of computers, networks, or databases within the victim organization, making the attacker's job considerably easier. Credential theft may utilize password spraying, rainbow tables, brute force attacks, and other methods of password guessing.[9] Some organizations protect accounts with *multifactor authentication* that relies on multiple factors of identity such as a password, plus something the user has such as a token, personal identification number (PIN), mobile device, or possibly a biometric such as a fingerprint. Multifactor authentication makes credential theft considerably harder to execute, but still not impossible.

Malicious Websites and Malvertising

These cyberattacker techniques involve creating malicious web content intended to trick users and compromise vulnerable web browsers. Malicious websites may be designed to look like legitimate websites, prompting users to enter their usernames and passwords for the purpose of *credential theft*. Malvertisements may be designed to coax users to visit malicious websites, or simply attempt to use *exploits* to compromise vulnerable web browsers. Malicious websites may also seek to get users to install *malware* by offering enticing content like pirated movies, free music, or dirty pictures.

9 See the *Glossary* in this book for definitions of "password spraying," "rainbow tables," and "brute force attacks."

Phishing

This attack involves sending e-mail messages to victims, attempting to entice them to open attachments containing *malware*, or click on links to *malicious websites* or *malvertisements*. Phishing messages may be forged to appear to come from inside the organization, or may be targeted toward specific individuals with customized messages to make them more enticing. Messages may ask for personal information or ask people to give up their usernames and passwords to enable *credential theft* by the attackers. Targeting specific individuals is often called *spear phishing*. Specifically targeting organization executives is sometimes called *whaling*. Phishing has become the most commonly used and most effective method for attackers to gain access to victim organization computer systems.

Social Engineering

This attack involves using alternative, possibly "old-school" methods to gain entry to target organizations. For example, attackers may impersonate employees on the telephone or may call unsuspecting users to tell them their computers are infected with malware. Attackers may "dumpster dive" at target organizations to try to find papers containing account numbers or user credentials. Attackers may even attempt to gain physical entry to the victim organization by tailgating at access-controlled doors or by talking their way past front-door reception staff. Kevin Mitnick, in *The Art of Deception*, explains how he was able to use social engineering to successfully defeat the security of even large, sophisticated, organizations.[10]

Supply Chain and Internet of Things (IoT)

These attacks target victim organizations through vulnerable partners, third parties, and network-connected IoT devices. For large organizations with comprehensive cybersecurity programs, these attacks may bypass the organization's primary defenses by concentrating on smaller partner and third-party organizations who might not be as well-defended. Similarly, even when organizational personal computers are well-protected, internet-connected devices like phones, printers, video conferencing systems, thermostats, lighting controls, and even fish tanks may be

10 Mitnick, Kevin. *The Art of Deception: Controlling the Human Element of Security*, Wiley Publishing, Inc., 2002.

vulnerable and exploitable. There have been numerous cases where IoT devices were vulnerable brand-new from the factory, or even compromised while they were being manufactured within the source factory, and then connected to trusted organization networks. When this occurs, attackers can get past organizations' primary defenses and obtain network access without having to bypass a single organizational protection.

Accomplishing Hacker Goals

This list is just a sampling of the tools and techniques available to the well-equipped modern attacker. Frequently, attackers use combinations of these methods to penetrate large or complex organizations, taking days, weeks, or months from their first efforts until their eventual success. Professional cybercriminals and nation-state attackers, in particular, tend to be patient and persistent in their efforts. They will work diligently to bypass cyberdefenses, one at a time, in pursuit of their ultimate objectives. For this reason, organizations must be attuned to the concepts of *persistence* and *dwell time*, and must take seriously the possibility that, at any given time, attackers may already be in their midst, just waiting to make their move when the time is right.

What Do Real-World Cyberattacks Look Like?

When real-world attackers use real-world hacking methods, their attacks tend to fall into a number of consistent, well-defined patterns. These patterns involve aligning the abilities of the attackers with the vulnerabilities of the victims and the corresponding target objectives with regard to confidentiality, integrity, or availability. Of course, the attacks also frequently involve a monetary objective. Figure 2.3 lists some of the most common real-world cyberattack patterns.

Commodity Malware and Random Attacks

These attacks involve malware such as viruses and Trojans that are regularly circulating the internet, as well as automated servers that regularly scan the internet for unpatched and vulnerable devices. In 2004, the SANS Institute's Internet Storm Center, which monitors malicious internet activity, found that an unpatched Windows XP computer would be compromised within 20 minutes if it was connected directly to the internet without any other protections. These

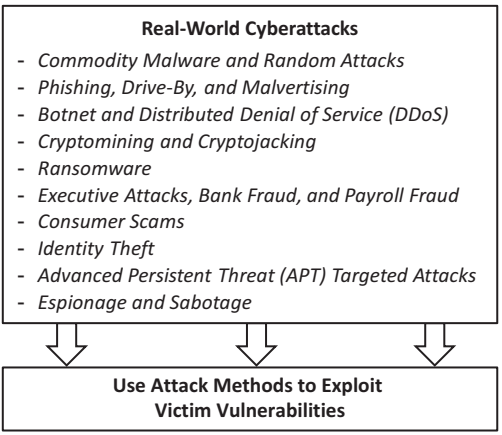


Figure 2.3: Real-world cyberattacks align attack methods against victim vulnerabilities to achieve specific objectives.

commodity attacks are constantly circulating and scanning, looking for vulnerable hosts to infect.

Phishing, Drive-By, and Malvertising

These attacks involve using phishing e-mails, malicious websites, and malicious web content to compromise unsuspecting users, computers, and devices. While slightly more targeted than commodity attacks, these attacks are also wide-ranging, with commodity phishing e-mails being sent daily to billions of users around the world. Malvertising at popular websites can similarly target millions, and even small success rates for these attacks can translate into large numbers of compromised hosts. These compromised systems can then be exploited further by the attackers.

Botnets and Distributed Denial of Service (DDoS)

Once vulnerable computers are compromised, they may be networked and put under an attacker's central control to create a *botnet*. Such botnets can be used to support DDoS cyberattacks that overload IT systems with a massive surge of network traffic that the victim's infrastructure is unable to handle. Botnets serve many purposes for attackers, including spam, command-and-control, malware

delivery, cryptomining, and DDoS attacks. The largest botnets include tens of millions of compromised computers worldwide.

Cryptomining and Cryptojacking

Once hosts are compromised, attackers can monetize the hosts by using them to create cryptocurrency, or "cryptomining." The anonymity and non-traceability of cryptocurrencies makes these attacks particularly attractive. Hijacking victim computers for cryptomining is often called "cryptojacking." While one computer cryptomining in the background does not tend to generate much revenue, tying thousands of compromised computers together can enable attackers to make serious money. This is especially true when cryptocurrencies such as bitcoin are worth thousands of dollars per coin.

Ransomware

Similarly, targeted users and organizations may be held hostage by ransomware. Ransomware works by encrypting the hard drives and data of compromised computers, and then demanding payment for the key to decrypt the hard drives and data. More sophisticated ransomware also encrypts or deletes backup copies of data, including file servers and cloud backups. Ransomware can be particularly effective when it targets individual personal computers that are not backed up, or when it targets entire organizations and takes large portions of their computers, servers, and infrastructure offline. Frequently, it is cheaper to pay the ransom than to rebuild. Of course, sometimes the ransom payment does not actually work, and the victims must rebuild anyway.

Executive Attacks, Bank Fraud, and Payroll Fraud

These attacks involve targeting organization executives, bank accounts, and payroll processes, with the goal of stealing money from organizational bank accounts. Executives may be impersonated online, with fraudulent orders sent to subordinates directing them to make bank transfers or payments. Attackers may target organizational bank accounts and attempt to directly withdraw funds, or compromise payroll systems to change direct deposit information. These attacks can often steal thousands or even millions of dollars

before they are detected, and organizations may have only limited recourse with their banks after the money is gone.

Consumer Scams

These attacks involve targeting consumers to get them to give up personal information like e-mail addresses or online accounts, or to get them to directly pay the attackers for fraudulent services such as computer repair, anti-virus installation, or telephone support. While not as lucrative as organizational attacks, these attacks can target unsuspecting users (such as children and the elderly) and may have higher success rates due to lower victim awareness.

Identity Theft

This attack involves targeting identity information such as home addresses, e-mail addresses, account logins, credit card numbers, bank account numbers, and health care records. Some of this information (such as bank accounts) can be directly exploited for money, but more often, identity information is then sold on the black market to aggregators. The aggregators collect personal and account information for millions of individuals and then use the information to drive entire campaigns of fraud and theft.

Advanced Persistent Threat (APT) Targeted Attacks

These attacks involve highly specialized cyberattacks designed to penetrate even the most ardent cyberdefenses for major corporations and government networks. These attacks are frequently nation-state sponsored, but increasingly, the same tools and techniques are being used by professional cybercriminals as well. Key to an APT attack is the factor of time. An APT attacker may take days, weeks, or months to fully penetrate their target and achieve their objective. These attackers attempt to defeat one layer of cyberdefense at a time, and may wait days or weeks for a “lucky break” to get past specific defensive measures. These lucky breaks may include unpatched software, flawed applications, insecure accounts, or holes in network defenses. APT attackers frequently get to their objectives by obtaining systems administrator access so they can bypass or disable other defenses. They may also attempt to be stealthy in order to stay “under the radar” and keep defenders blind to their persistent presence.

Espionage and Sabotage

These attacks involve penetrating victim networks to steal sensitive and proprietary information, or damage IT or physical systems. While these are often the objectives of nation-state and military attackers, they may also be the objectives of commercial cyberattackers seeking to steal competitors' techniques or technologies, or to hamper their businesses. These attacks frequently use APT techniques but may also be opportunistic, depending on the countries involved. Examples of these types of cyberattacks include activities by North Korean cyberattackers against Sony Pictures and other targets, as well as the ongoing cyber campaigns involving Russia and the Ukraine.

Exploiting Victim Vulnerabilities

While this list covers many types of common cyberattacks, it is far from a comprehensive list. Real-world cyberattacks may include blends of the cyberattack types listed here, reflecting a complex array of people, services, businesses, and technologies. Nation-state cyberattackers may buy access to targets from criminal cyberattackers, while hacktivists may employ established botnets to perform politically motivated DDoS attacks. System administrators may make mistakes, resulting in public breaches that are then exploited by cyberattackers and criminals for profit or gain. Hackers may even hack other hackers, further exploiting the victims to accomplish their goals.

How Do Cyberdefenses Counter Attacks?

To thwart cyberattacks, defenders have a number of tools in their arsenal. The old adage goes that "the attacker just has to succeed once, while the defender has to succeed every single time." While there is some truth to this adage, the reality is not as hopeless as the expression may imply. A successful cyberdefense can thwart attackers while also being resilient enough to continue working after some (or even most) of the cyberdefenses have failed or been defeated. Designing comprehensive, robust, and redundant cyberdefenses is part evidenced-based (i.e., part science) and part experience-based (i.e., part art). Figure 2.4 lists some of the cyberdefense functions that can be used to counter cyberattacks.

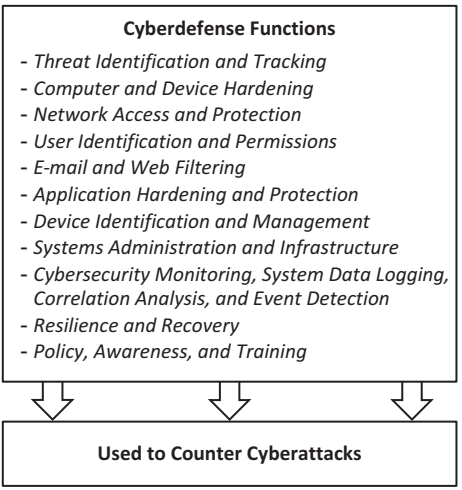


Figure 2.4: Successful cyberdefenses can thwart attackers and continue working when some cyberdefense functions have failed or been defeated.

Threat Identification and Tracking

This function involves identifying and tracking the cyber threats to the organization. Cyber threats may be characterized by indicators of compromise (IOCs) that identify malicious attacker activity in an organization. IOCs may include attacker accounts, computers, or network addresses that are identified using forensics. Cyber threats may also be characterized by attacker tools, techniques, and procedures (TTPs) to include communications patterns, file hashes, or network protocols. IOCs and TTPs can be used to generate cybersecurity alarms or alerts on a detection system. An alert indicates an incident is occurring and requires investigation and follow-up. IOCs and TTPs may be obtained from open sources – referred to as *open source intelligence* (OSI) – or provided by proprietary threat intelligence information feeds and services.

Computer and Device Hardening

This function involves hardening individual computers and network-connected devices to make them more difficult to compromise with malware. Anti-virus software is a common hardening technique, but is hardly the only approach. Hardening may include using security technical implementation guides (STIGs) that specify security settings to configure and enable the most important computer and device

security features. These features may include specific security policy settings and system monitoring to detect potentially malicious activity and malware.

Network Access and Protection

This function involves configuring computer networks to block potentially malicious access, restrict potentially malicious network traffic patterns, and detect potentially malicious network activity. Many technologies may be involved in network protection. Some of the more common network protection techniques include secure configuration of routers and switches, installation of firewalls, network intrusion detection systems and intrusion prevention systems (IDS/IPS), access control gateways, and virtual private networks (VPNs). Network segmentation, which involves isolating network sections to enforce security boundaries, is a particularly powerful network protection technique when properly employed.

User Identification and Permissions

This function involves identifying, authenticating, and authorizing user access across the organization when accessing organizational networks, computers, and applications. Sometimes these activities are called *identity and access management* (IAM), though most people recognize it by usernames and passwords. Cloud is making IAM increasingly important, as many cloud services are only protected by user accounts, and the compromise of a single user's credentials may enable unfettered access to the cloud service. By properly identifying users and limiting their access permissions, the organization can restrict access and limit cyberattack damage, while also creating audit trails that can be critical to cyberattack investigation.

E-Mail and Web Filtering

This function involves identifying and filtering e-mail and web traffic into and out of the organization. For most organizations, e-mail and web browsing are the two main ways information enters and leaves the organization, as well as the main avenues for the delivery of malicious links, web pages, and software. By analyzing and filtering this traffic, the organization can filter out unsolicited spam, many types of malware, and block access to inappropriate and malicious websites. While hardly 100% perfect, aggressive filtering can dramatically reduce the amount of malware entering the organization on a daily basis.

Application Hardening and Protection

This function involves protecting the organization's software and applications from compromise and malware. It may include protecting software on computers and devices, software running on internet-facing servers, and custom-developed software used inside the organization. This function includes deploying patches to update software, and identifying and remediating software vulnerabilities as they are discovered and where appropriate. It may also include management of cryptography and keys used to encrypt data or authenticate communications. Sometimes, software vulnerabilities cannot be patched, or are inherent in how the software operates. When this situation is the case, other security functions like network protection may be needed to compensate.

Device Identification and Management

This function involves identifying and tracking the devices (particularly the network-connected ones) used in the organization, and then managing those devices to ensure their safety and security. Modern network-connected devices have a mind-boggling level of capabilities: system on a chip (SoC) processors with networking and cryptography built-in; wired, wireless, and Bluetooth networking; and onboard flash and hard drives with gigabytes or even terabytes of storage. This functionality comes with risk, as these systems are seldom updated after they leave the factory, and even lowly telephones and fish tanks[11] have become avenues for cyberattack and infection. By tracking and managing these systems, organizations can understand these vulnerabilities and choose appropriate mitigations where possible.

Systems Administration and Infrastructure

This function involves protecting the "behind-the-scenes" IT systems that underly and support the organization's other, more visible endpoints, servers, networks, and applications. Because these systems are not directly visible, they often receive little cybersecurity attention and may become the "soft underbelly" of the organization. Poor systems administration and infrastructure security can expose the organization to devastating cyberattack from hacktivists, professional

11 Schiffer, Alex. "How a fish tank helped hack a casino," *The Washington Post* (July 21, 2017).

cybercriminals, or APT attackers. By giving these systems special attention and protecting them with cyberdefenses – including monitoring, multifactor authentication, and network isolation – the organization can dramatically reduce its vulnerability to advanced attacks.

Cybersecurity Monitoring, System Data Logging, Correlation Analysis, and Event Detection

This multifaceted function involves putting cybersecurity capabilities in place to detect cyberattack activity, and taking action when those capabilities indicate signs of malware or attacker activity. This function involves monitoring organization systems, collecting system log data, correlating cybersecurity events or alerts, and detecting malicious cybersecurity behavior or events that warrant investigation. Monitoring may be placed on networks, endpoints, applications, user accounts, and even databases to detect signs of cyberattack. While it may be helpful to detect attacker activity against the organization's outer perimeters, it is critically important to be able to detect attacker activity that has penetrated initial lines of defense and is operating inside the organization's networks, devices, and user accounts. By monitoring networks, devices, and user accounts, logging important activity, and correlating alerts, the organization can detect attackers and stop them before they can succeed in their attacks.

Resilience and Recovery

This function involves the organization building out capabilities to respond, recover, and rebuild after damage is caused by a cyberattack. Cyberattacks do not have to succeed to cause damage, as a failed cyberattack may leave accounts locked, networks disabled, or computers infected. The organization must have the ability to take systems offline for attack containment and recovery, while still permitting business to continue during recovery. Capabilities to support resilience and recovery may include system redundancy, alternate locations, offline backups, and code repositories. While such systems may also be used for protecting against operational failures, cyberattacks are different from burned-out hard drives or network outages, and should receive special attention when designing protections.

Policy, Awareness, and Training

This function involves making sure the people of the organization (and its partners, contractors, and consultants) understand the organization's cyberdefense objectives, and are prepared to do their parts to support those objectives. Cybersecurity cannot occur in a vacuum, and regular employees being cyberaware can dramatically reduce the pressure on the organization's cybersecurity staff. Everyone should understand the organization's cybersecurity threats and risks, how security protections reduce those risks, and the importance of individual actions in helping those protections to work, or at least not undermining them.

Countering Cyber Attacks

By deploying cyberdefense capabilities to fulfill these functions, organizations can build robust cyberdefenses that can resist attack from a wide range of attackers. Cyberdefense functions work together, and it is uncommon for a cyberdefense built around a single function to resist cyberattack for very long. Successful cyberdefenders build cyberdefenses that employ multiple functions – or even all of them – together in concert to create a robust defense.

Choosing and Prioritizing Cyberdefenses

At the 2019 RSA conference[12] in San Francisco, CA, there were approximately 550 companies exhibiting their cybersecurity technologies, solutions, and services, along with approximately 50,000 attendees. This conference presents an impressive array of companies and capabilities that can contribute to an organization's cyberdefense. *Which are the most useful capabilities? Which capabilities are the best value? Are any of the capabilities truly the "silver bullets" that their marketing materials claim?*

To best choose cyberdefenses, organizations must understand what assets need to be protected, the vulnerabilities of assets when protections fail or are missing, the threats that may jeopardize assets, and how protections and defenses (i.e., countermeasures) can reduce the risk of threats. From that information, organizations can make smart business decisions about what defenses will be most effective while also making sense from a business perspective. This process of choosing cyberdefenses involves *cyber risk management*, which is the topic of Chapter 3.

12 RSA is an annual cybersecurity conference hosted by the RSA company. The acronym "RSA" refers to the founders of the company, Ron Rivest, Adi Shamir, and Leonard Adleman.

Chapter 3
Cyber Risk Management

Cyber risk management is a systematic process for analyzing how an organization could succumb to cyberattacks, and explores options for reducing either the likelihood or the impact of the attacks that occur. *Cyber risk analysis* involves performing an integrated set of activities, according to a risk management process, to identify potential security compromises, their consequences, and ways to mitigate them.

Cyber Risk Management Process

While there are a number of risk management processes, they generally involve performing the steps shown in Figure 3.1.

Figure 3.1: This simplified cyber risk management process shows an analytical progression from assets to countermeasures designed to determine and reduce an organization's risk profile.

The risk management process identifies *assets*, *vulnerabilities*, *threats*, *risks, risk severity*, associated *risk treatments*, and *countermeasures*. Risk severity is measured in terms of *risk likelihood* and *risk impact*. These *key terms* are defined as follows:

- *Assets* are anything of value to an organization or to attackers. For example, social security numbers, computers, and servers are all assets, along with customer databases and proprietary intellectual property.
- *Vulnerabilities* are weaknesses that attackers may exploit to harm one or more assets that an organization cares about. For example, computer operating systems may have vulnerabilities due to missing software updates or patches, or web sites may have vulnerabilities in their underlying code.
- *Threats* are the ways attackers exploit vulnerabilities to cause damage to organizational assets. For example, one type of threat is computer viruses infecting organizational computers due to missing software updates or patches.

https://doi.org/10.1515/9781501506529-003

- *Risk* is the potential damage to assets, causing an impact to the organization. For example, a risk can be when attackers use compromised computers to steal data, embezzle money, or take critical systems off line.
- *Risk likelihood* refers to the likelihood that the risk will manifest itself, resulting in a consequence. For example, likelihood could be characterized in terms of low likelihood (unlikely to occur), medium likelihood (possible to occur), or high likelihood (likely to occur).
- *Risk impact* refers to how great the consequence of the risk is to the organization's business and priorities. For example, the risk could have a low impact (a slight effect), a medium impact (a moderate effect), or a high impact (a significant effect).
- *Risk severity* is determined by combining the *risk likelihood* and *risk impact* of each potential threat into an "overall" risk level – a risk severity level. This risk severity level can then be used to prioritize risks and consider potential risk treatments. For example, a risk that is characterized as being low risk (unlikely to occur), but having a high impact (significant effect) on the organization might be assigned an overall risk severity level of "medium." The risk severity level can then serve as a starting point for further analysis and prioritizing of the risk alongside other identified and characterized risks.
- *Risk treatments* are ways to reduce risk besides just trying to prevent the risk from happening. For example, an organization can "avoid" the risk by eliminating the vulnerability or threat, or it can "reduce the likelihood" of the risk manifesting itself through cyberdefenses, or it can "reduce the impact" by purchasing cyber insurance.
- *Countermeasures* are security protections designed to reduce risk by eliminating vulnerabilities or countering potential threats. For example, an organization can implement cybersecurity controls to "reduce the likelihood" that the risk will occur by blocking potential cyberattacker activities.

Security professionals perform the cyber risk management process within the context of applicable cybersecurity drivers[1] that include the following: (1) laws and regulations, (2) cybersecurity standards, (3) contractual obligations, and (4) liability and insurance. Security professionals should be interested in identifying and addressing the most pressing organizational risks, while understanding that risk can be reduced but seldom eliminated. Risk management involves balancing factors of cost, convenience, and speed to find ways to reduce risk without getting in the way of the organization too much. Remember, there is no perfect cyberdefense.

1 See Chapter 5, "Cybersecurity Drivers," for a detailed explanation.

Figure 3.2 shows additional details for the six-step cyber risk management process introduced in Figure 3.1.

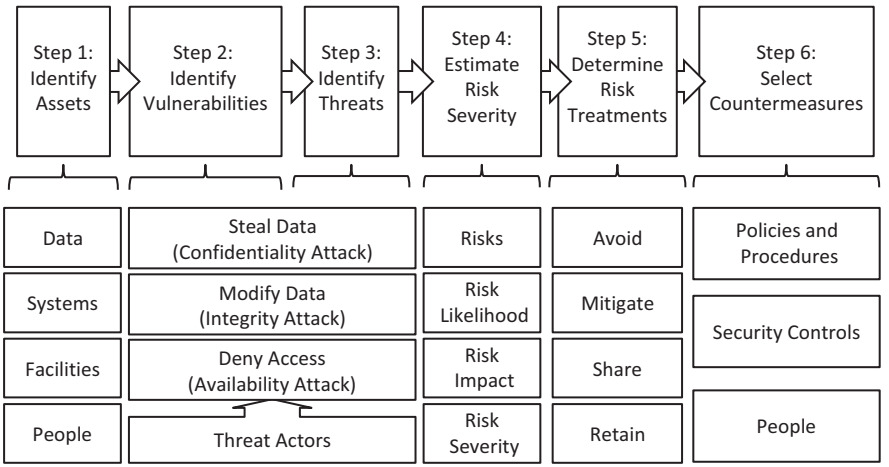


Figure 3.2: This detailed cyber risk management process depicts the major steps from Figure 3.1, with additional detail showing major considerations for each step.

The following pages describe the cyber risk management process in terms of its major steps and activities within each step. Simple examples are included to provide additional insight to the concepts described.

Step 1: Identify Assets

The first step in the cyber risk management process identifies and inventories the *assets* that are of value to the organization and should be protected. As shown in Figure 4.2, assets can include the following:

- *Data* is the information held by the organization, whether it is proprietary, customer, organizational, vendor, or personal data.
- *Systems* use processes, procedures, and data to accomplish organizational or personal goals.
- *Facilities* are the locations where people in the organization work, or a person or family resides, and the tools and equipment at those locations.
- *People* are the organization's personnel, partners, or family members, along with their knowledge and abilities.

These are not the only asset types, but these categories can be used as a starting point for analysis. For example, an organization may consider other asset types such as *vendors, relationships, reputation*, *processes*, or other critical *information*. Each organization needs to identify and track assets that make sense for its particular situation.

Organizations must also make value decisions regarding their assets. While most organizations will tell you, "Our people are our most valuable asset," organizations must constantly manage resource allocation tradeoffs regarding their data, systems, facilities, and people – that is, what and who gets organizational resources. These assets must be protected to varying degrees, and resources must be traded off among them to provide protection that is effective but balanced with other organizational resource priorities.

Organizations must also consider the value of their assets. *Do you treat a pair of $10 generic sunglasses the same as a pair of $100 designer glasses?* Probably not, since the cheap glasses are easily replaced. *Do you protect your address like you protect your social security number?* Probably not, since your address is on the front of your house or building. *Do you worry about a leaky roof in your shed the same way as one in your bedroom?* Probably not, since a little water in an outdoor shed likely isn't going to damage much. By considering asset *value*, organizations can make more intelligent decisions about which assets are more valuable and, consequently, more worth protecting.

Step 2: Identify Vulnerabilities

The second step in the cyber risk management process identifies *vulnerabilities* that could be exploited by threats or threat actors to harm the assets that organizations care about. Unfortunately, it is common in risk management for bad things to occur because a vulnerability is not identified or is inadequately addressed. The most common vulnerabilities are software vulnerabilities in operating systems and application programs; these vulnerabilities are often remediated by installing patches. These types of vulnerabilities can be detected using vulnerability scanners such as *Metasploit* or *Nessus*. However, missing software patches are hardly the only types of vulnerabilities in modern IT systems.

Vulnerabilities not related to missing patches tend to be aligned to both assets and threats. While assets and threats can be considered somewhat methodically, vulnerability considerations may require a bit more creativity. A useful technique in identifying vulnerabilities is to consider *consequences* that may occur when a vulnerability has been exploited, or when a protection fails or is

missing. As depicted in Figure 3.2, cyberattacks have several major goals that include the following:

- *Confidentiality attacks* seek to *steal data* that is valuable and should be kept confidential. Such data might include account passwords, social security numbers, credit card numbers, bank account information, electronic health records, organizational secrets, or executive correspondence. Attackers may seek to directly use this confidential information, or their objective may simply be to collect it and sell it on the "dark web" criminal internet.
- *Integrity attacks* seek to *modify data* to cause disruption or harm. These attacks may include changing accounts or passwords, creating fraudulent transactions, or stealing money out of bank accounts. Such attacks can harm an organization's or individual's welfare, self-confidence, financial situation, or reputation.
- *Availability attacks* seek to *deny access* to systems, services, or data by making them unavailable to the people who need them. These attacks may include shutting down applications, deleting or encrypting data, or even causing physical harm to computers, devices, or industrial equipment. Systems and data that are disabled may need to be recovered, rebuilt, or even replaced.

In the above list, *confidentiality*, *integrity*, and *availability* (CIA) are terms used by cybersecurity professionals to talk about how information can be exploited and how information systems may be vulnerable to attack. *Confidentiality* refers to protecting information that should be kept secret so that it is not stolen or disclosed. *Integrity* refers to protecting information from being changed to prevent fraudulent transactions or deleting logs of criminal activity. *Availability* refers to ensuring that information is available when it is needed and that those who need it are permitted to access it.

Vulnerability analysis involves considering situations where something occurs that makes the chance of a threat manifesting itself greater than "normal." For example, walking on the sidewalk might not be considered a "vulnerability," even though there are lots of ways that something bad could happen while walking on the sidewalk. However, jaywalking across a busy road might represent a significant vulnerability, both because of the obvious danger and also because it is illegal. Vulnerability might be present when a door that is normally locked is left unlocked, or a sensitive computer is connected to a public network, or third parties are allowed into our homes or offices. An organization will want to apply these types of mindsets to its IT systems, to identify vulnerabilities related to how systems operate, how they interact, and how they interconnect.

A vulnerability increases the likelihood that something bad might happen.

Step 3: Identify Threats

The third step in the cyber risk management process identifies the *threats* that may jeopardize organizational assets. Threats frequently revolve around *threat actors* who may wish to do us harm. Threats may be natural or man-made, accidental or deliberate, random, or deterministic. Threats are the ways in which vulnerabilities can be exploited to cause damage to assets. Identifying threats involves a lot of Murphy's Law thinking – *What can possibly go wrong?* Examples of threat actors and threats that an organization may want to consider include the following:

- *Carelessness* that includes mistakes and negligence, that can cause security to be compromised, data to be exposed, or systems to be disabled.
- *Commodity threats* that include random malware, viruses, worms, and botnets. Commodity threats may exploit vulnerabilities or other cyberdefense weaknesses, but they do not usually adjust or adapt to work their way around protections that are in place.
- *Competitors* looking to steal business or gain an advantage.
- *Customers* with whom organizational relationships are not always good.
- *Cybercriminals* have found that there is serious money to be made on the internet. Cybercriminals seek to gain access to computers, accounts, and networks, then exploit the access to either directly steal money or steal data that can then be quickly and easily turned into money.
- *Cyberterrorism* is conducted using similar techniques as cybercrime, but by unaffiliated individuals or terrorist organizations. Cyberterrorism is done for an activist agenda, or it may simply be performed for the sake of anarchy and destruction for its own sake.
- *Cyberwar* is about damaging the ability of organizations or governments to operate in cyberspace. This damage is done by overwhelming, overloading, disabling, or destroying the IT systems used by the victims, or even using those IT systems to cause physical systems to malfunction and damage themselves or their operators.
- *Espionage* takes cybercrime to the next level, but is generally focused on stealing information. Cyberespionage is more complex in its objectives and how it carries them out. Cyberespionage steals trade secrets, blueprints, formulas, software code, budgets, and project schedules for commercial advantage, or national secrets for political or military advantage.
- *Hackers* who want to control organization computers or accounts, and then exploit that control to serve their personal or organizational objectives.
- *Hacktivists* conducting targeted attacks to make a public or political statement. Their goal is to use hacking to bolster their cause or embarrass their

adversaries. They are seldom out to hurt anyone or do significant physical damage. Most often, hacktivists are simply looking to get their message out and draw attention to their cause.
- *Insiders* who may be employees or trusted third parties who want to steal from or sell out the organization.
- *Nature* should never be underestimated as it can destroy facilities, disable personnel, and disrupt operations.

In these examples, threats can cause harm or damage to assets, either directly or indirectly: a criminal can steal money, a hacker can take over computers, a competitor can steal trade secrets, an insider can pilfer goods, a mistake can harm customers, angry customers can tarnish an organization's reputation, or an act of nature can disrupt operations. In these cases, a threat or a threat actor can take an action that jeopardizes something of value to the organization.

How significant a threat really is depends both on the severity of the threat, as well as the value of the asset. While most of us are not too concerned about a criminal stealing our beach towel, most of us would be very concerned if a criminal were to steal our car. How often have we left something outside at our home or business, thinking to ourselves, "Nobody would take *that*." *Conversely, how many of us roll up our windows and lock our doors when we park our cars in a parking lot? What actions do we take to "batten down the hatches" at home or work when we know that a storm is coming?* We analyze threats every day.

Step 4: Estimate Risk Severity

The fourth step in the cyber risk management process estimates the *risk severity* for the threats that are of concern to the organization. When estimating risk severity, it is helpful to start the process by constructing *risk statements* using the assets, vulnerabilities, and threats that were identified in the preceding three steps, along with a corresponding c*onsequence* that the organization cares about. The risk statement describes the risk in plain language that can be easily understood and can be further analyzed as necessary. The following sentences are examples of potential day-to-day risk statements:
- A criminal steals your driver's license and credit card because you left them lying out, causing you inconvenience.
- A rainstorm leaks through a broken window, causing water damage to office computers.
- An employee inadvertently posts customer data to a public website, resulting in a breach of confidential personal information.

- Customers get away with shoplifting merchandise because of poor inventory management, costing the business money.
- Ransomware installs itself on your unpatched internet-connected computer, destroying your valuable photos and documents.

Each of these risk statements identifies a risk in terms of assets, vulnerabilities, threats, and consequences:

- *Assets* include credit cards, computer data, confidential customer information, merchandise, and office computers.
- *Threats* include criminals, hackers (ransomware), careless employees, customers, and acts of nature.
- *Vulnerabilities* include leaving things lying around, missing patches, poor data protection, poor inventory management, and broken windows.
- *Consequences* include inconvenience, loss of valuable data, breach of confidential data, loss of revenue, or property damage.

Once risk statements have been constructed, the risks themselves can then be considered in terms of two properties: *likelihood* and *impact*.

- *Likelihood* refers to how likely it is that the risk will manifest itself, resulting in a consequence. A high likelihood risk may occur daily, weekly, or even more often, while a low likelihood risk may typically occur less than once in a lifetime.
- *Impact* refers to how great the consequence of the risk is, in the grand scheme of things. A high-impact risk may result in a loss of life or may jeopardize the existence of a company, while a low impact risk may only be an inconvenience, cost a few dollars, or result in a small mess to clean up.

Figure 3.3 illustrates one way in which *risk likelihood* and *risk impact* can be combined into an overall risk level or *risk severity*.

		Risk Impact		
		Low (Risk has *slight* effect)	**Medium** (Risk has *moderate* effect)	**High** (Risk has *significant* effect)
Risk Likelihood	**High** (Risk *likely* to occur)	**Medium**	**High**	**High**
	Medium (Risk *possible* to occur)	**Low**	**Medium**	**High**
	Low (Risk *unlikely* to occur)	**Low**	**Low**	**Medium**

Figure 3.3: Risk severity can be determined by combining risk likelihood and risk impact.

Likelihood and impact can both be analyzed to (1) understand how great the risk really is, (2) group risks by their relative severity, and (3) provide input to budgetary and investment decisions. Security and IT professionals, among others, can provide their "expert judgment" regarding risk likelihood and risk impact, as follows:

- *Low severity risks* might be those risks with a low likelihood and a low impact. Low severity risks are often categorized as a low-priority budget investment, and frequently may be accepted, without mitigation.
- *Medium severity risks* might be those risks with a high likelihood and a low impact, or a low likelihood but a high impact. Medium severity risks often require further analysis to understand the risks so that management can decide what needs to be done to mitigate them.
- *High severity risks* might be those risks with a high likelihood, and a high impact. High severity risks should be given priority for mitigation and have their severity reduced through treatments or countermeasures.

While risk analysis and evaluation can be done at any level – using either more or fewer levels of detail – this general framework of *low*, *medium*, and *high* is robust and good enough for most organizations. Grouping risks by "severity" helps an organization determine appropriate risk treatment strategies.

Step 5: Determine Risk Treatments

The fifth step in the cyber risk management process determines the *risk treatments* for the identified risks. Not all risks can be mitigated, especially when cost is a consideration. Similarly, even risks that can be significantly reduced can seldom be eliminated completely. For example, some risks may have to be accepted as a "cost of doing business," such as the chance of occasional shoplifting when operating a convenience store. Other risks, like natural disasters or acts of war, are simply far outside an organization's ability to control in any way. However, organizations can reduce risk by using the following risk treatments:

- *Avoid* the risk by eliminating the vulnerability or the threat.
- *Mitigate* the risk by reducing the likelihood that it will occur or the impact when it does occur.
- *Share* the risk by introducing a third party (such as an insurance company or a security service) that compensates the organization in the event that the risk occurs.

– *Retain* the risk, where the organization simply accepts the possibility that the risk may occur and deals with the consequences when it happens; self-insurance is a good example of this strategy.

Perhaps the most interesting risk treatment involves *sharing the risk*. While the term "sharing" sounds like this treatment is referring to some type of partnership arrangement, it usually involves purchasing insurance or some type of contract arrangement that pays in the event of a breach. Sometimes, cybersecurity services may include similar payments in case their service fails to perform as expected or it is defeated by an attacker.

When an organization purchases insurance, it is sharing the risk with the insurance company. The insurance helps an organization contain the risk and reduce its exposure and potential loss. Of course, that is provided the insurance company does not go bankrupt, which is usually a risk that an organization would simply *accept*. Interestingly, the insurance company may then require that an organization take other actions to reduce its risk. For personal insurance, this requirement might include properly maintaining your car or having smoke detectors in your house. For cyber insurance, this requirement might include installing certain cybersecurity protections on an organization's IT systems.

Regardless of the specific risk treatment strategy, risk treatments can help an organization to subsequently identify and select *countermeasures* to help mitigate organizational risks where mitigation is appropriate.

Step 6: Select Countermeasures

The sixth step in the cyber risk management process identifies and selects *countermeasures* designed to reduce the likelihood or the impact of identified risks. Countermeasures can include security policies and procedures, security controls, and people.

Countermeasure Policies and Procedures

Countermeasure policies and procedures define required organization cybersecurity behavior. Policies define what is to be protected and to what degree, along with organizational responsibilities. For example, a countermeasure policy may require data in motion or data at rest to be encrypted. Such an encryption policy might help to protect data from unauthorized access when organization laptops

are lost or stolen. Countermeasure procedures supplement policies and consist of step-by-step actions to reduce or eliminate security vulnerabilities and threats.

Effective countermeasure policies and procedures should be written and disseminated so that employees are aware of what constitutes authorized and unauthorized security behavior, along with the consequences for non-compliance. Organizations should provide countermeasure training so employees understand their specific responsibilities and duties.

Security Controls

Security controls[2] are applied to an IT system or business process to prevent, detect, or investigate specific activities that are undesirable, and respond to those activities when they occur. Some security controls are mandated by law or regulation, such as wearing your seat belt in a car or having auto insurance. Other security controls are "industry best practices," such as those used by the government, a bank, or an e-mail provider. Security controls can reduce risk by preventing and detecting bad behavior, or helping to seek out and investigate when something bad has occurred.

Security controls include the following types:

- *Preventive controls*. Block undesired activities and prevent them from occurring.
- *Detective controls*. Generate alerts on suspected attacker activity that can then be acted upon.
- *Response controls*. Activated after detective controls "alert" cyber personnel of suspected attacker activities, and assist defenders in investigating the alert, identifying the cyberattack, containing the attacker, and ultimately repelling the attack.
- *Recovery controls*. Engaged to close out cyber incidents and restore normal operations.

Security controls can have the following capabilities:

- *Reduce likelihood*. Controls can reduce how likely it is for the risk to occur, or can make it more difficult for attackers to execute on the risk.
- *Reduce impact*. Controls can reduce the impact when the risk does occur, perhaps by limiting the amount of damage that occurs.

2 See Chapter 4, "Cyberdefense Concepts," for a detailed description of cyberdefense security controls.

- *Detect occurrence*. Controls can detect the occurrence of the risk happening, allowing for an active response to thwart the attack, contain the damage, and reduce the potential exposure.
- *Collect evidence*. Controls can collect evidence that is used to show the operation of security controls, detect failures of the controls, or support investigations after an incident has occurred.

It is important to consider how security controls interact with each other and how they serve useful purposes individually and as a system. Ideally, all four control types will be used together to deliver capabilities that comprehensively mitigate the organization's cyber risks.

People

People involved with security countermeasures include employees, partners, and contractors authorized to have specific access to organizational assets. Authorized employees include executives, IT staff, and security staff. Security and IT professionals should have the knowledge, skills, abilities (or KSAs), and industry-accepted certifications required to carry out their day-to-day security responsibilities.[3] Similar comments can be made regarding contractors, third-party organizations, or subject matter experts hired to support an organization's cybersecurity program.

An organization's actual security against a professional attacker is almost entirely dependent on its people, not its technology.

Each of these countermeasures is interesting in its own way, but choosing which countermeasure or combination of countermeasures is appropriate depends on the nature of the risk itself. For example, we can avoid risks related to driving our car by changing routes, getting a safer car, or only driving at certain times. However, there may be certain risks that cannot be avoided. For example, criminals may visit an office building or a retail store that we are operating, and our actions are unlikely to change their intentions. Similarly, there are many risks in life that we simply accept and live with the consequences if they occur. Examples of this include getting mugged, losing our wallet, accidentally dropping our phone, or making a mistake at work.

---

3 See Chapter 11, "Cyber Training," for additional detail regarding organization cyber training.

On the other hand, cyberattack risks or losing valuable personal data probably warrant mitigation of some sort so that the risk can be reduced in either its likelihood or impact. Countermeasures may reduce the likelihood or the impact of the risk manifesting itself. For example, a lock on a door reduces the likelihood that someone is going to walk into your home in the middle of the night, though it will not reduce the impact should they break down the door and come in anyway. Having a backup of the data on your phone will dramatically reduce the impact if you accidentally drop it, but it will probably have little effect on the likelihood of that occurring. Similarly, cameras and alarm systems help us to detect when a break-in occurs, and can allow us to collect evidence that we can pass on to authorities who might investigate the crime. In the cyber world, computer logs and security alerts can serve a similar purpose for our computer systems.

Risk Registers

Organizations can use a *risk register* to document and track identified risks, along with their associated mitigations. At this point in the cyber risk management process, a systematic security analysis has identified assets, vulnerabilities, and threats. Risks have been identified and evaluated, and corresponding risk treatments have been determined. Security countermeasures have been selected and now need to be implemented. The risk register acts as a repository for tracking and managing these identified risks. Such registers can be implemented using a spreadsheet, database, or dedicated risk management software package. A risk register frequently contains data fields to include the following:

- *Risk identification number* uniquely identifies the risk.
- *Description of the risk* briefly characterizes the nature of the risk.
- *Risk likelihood* refers to how likely it is that the risk will manifest itself, resulting in a consequence.
- *Risk impact* refers to how great the consequence of the risk is, in the grand scheme of things.
- *Risk severity* based on an analysis of risk likelihood and risk impact.
- *Risk treatments* identifying if the risk is to be avoided, mitigated, shared, or retained.
- *Countermeasures* consisting of policies, procedures, security controls, and people.
- *Risk owner* who is the individual responsible for ensuring countermeasures are implemented for the identified risk.
- *Status* indicating the progress of the selected risk treatment for the identified risk.

Organizations may find that when they perform their risk management, there may be multiple risks that can be grouped together and addressed by a single countermeasure or security control. For example, when a person gets an umbrella insurance policy, that policy provides coverage to address a number of loss and liability scenarios. Similarly, there are many risks that may constitute "acts of nature" and are simply retained and may not require further analysis. In such cases, organizations may be able to use grouping to reduce the number of actual risk scenarios that need to be considered, and thereby simplify an organization's risk analysis. Risk registers can make such analysis and grouping of risks straightforward.

Wrapping Up: The Cyber Risk Management Process

Not all risks are created equal. Rather, some risks are more severe than others. Every day, we subconsciously perform risk management over and over again to keep ourselves, our families, and our workplaces safe. When we perform this risk management, we consider *assets*, *vulnerabilities*, *threats*, and *consequences* to identify *risks* and their *severity*, then *prioritize* risks so we can focus on the most important risks first.

When we have prioritized and identified our risks of greatest concern, we consider *risk treatments* and *countermeasures* that will help us address the risks and mitigate them to acceptable levels. Some risks we *avoid*; some risks we *insure* against; and some risks we simply *accept*. We may choose to mitigate other risks by reducing their *likelihood*, their *impact*, or by establishing *detection capabilities* to catch when risks occur so we can respond to them.

While individuals may do this risk management subconsciously on a day-to-day basis, organizations need to perform their risk management methodically and scientifically. Methodical risk management can involve large numbers of documents, spreadsheets, and databases that staff pore over to understand the nature of organizational risks, their consequences, and their mitigations. Organizations may create large databases to track risk characteristics, parameters, dollar values, associations, or other properties. As a part of this rigor, organizations may make tables of assets, risk statements, and countermeasures, and then use those tables to track their risk treatment efforts. By being conscious of the overall cyber risk management process, organizations can perhaps be more methodical in their analysis and can reduce their overall risk as well.

Chapter 4
Cyberdefense Concepts

Organizations face constant cyber threats, associated risks, potential security compromises, and the consequences of such compromises. Security professionals employ cyberdefense concepts to identify and mitigate cyber threats and risks. Different ways of looking at cyberdefenses shed light on how various "parts" fit together, how the parts overlay onto an organization's IT, and how the parts fit into an overall organization security framework. Figure 4.1 depicts some of the major cyberdefense concepts discussed in this chapter.

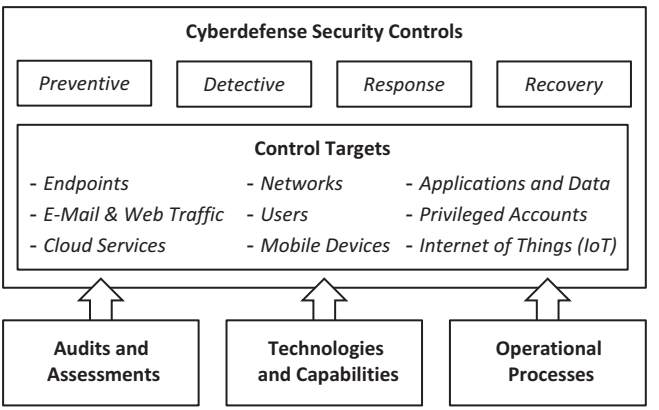


Figure 4.1: Defending against cyber threats and risks consists, in part, of integrated cyberdefense controls, control audits, control assessments, and cybersecurity technologies, capabilities, and operational processes.

This chapter describes cyberdefense concepts in terms of *cyberdefense security controls*, *audits and assessments*, *technologies and capabilities*, and *operational processes*. The chapter starts by defining what a control is and *nine* targets where controls can be applied: endpoints, networks, applications and data, e-mail and web traffic, users, privileged accounts, cloud services, mobile devices, and network-connected internet of things. The chapter then characterizes *four* types of cyberdefense security controls – *preventive*, *detective*, *response*, and *recovery* – and how each type of control might be performed against the nine control targets. The chapter also considers control *audits and assessments* to understand how controls

https://doi.org/10.1515/9781501506529-004

function and whether they are effective. The chapter closes by briefly introducing how *technologies and capabilities* and *operational processes* enable an organization to implement specific controls as part of its overall cyberdefense.

Cyberdefense Security Controls and Control Targets

A *control* is a way of providing some level of assurance that a particular behavior is or is not occurring within an organization. A cyberdefense control provides this capability with regard to IT systems, the users who access them, and the data within those systems. Cyberdefense controls are applied against specific IT systems, applications or users within the organization's IT environment, which we can call *control targets*.

As further described in the following chapter sections, cyberdefense controls work by preventing, detecting, responding, or recovering from malicious cybersecurity activity. These controls can be applied to the following control targets to identify and mitigate cyber threats and risks.

Endpoints

Endpoint security controls can be applied to computer operating systems within an organization's computers, servers, and smart devices. They may restrict users' ability to make changes to their computers or install software, detect unauthorized changes or malicious software installation, or support investigations and respond to malware installed on systems.

Networks

Network security controls govern network traffic within the organization's computer networks, as well as communications among the organization, its partners, and the internet. Network security controls can restrict or block potentially malicious network traffic from known bad websites, detect potentially malicious network traffic patterns, or support investigations and respond to malware operating on the organization's network. These controls can be applied to external networks, internal networks, and inter-network interfaces.

Application and Data Security

Application and data security controls permit the control of specific applications and the data upon which they operate. They can be designed to protect at the protocol level, software level, or data element level. These controls can block potentially malicious application behaviors or data accesses, detect potentially malicious behaviors without blocking them, or support investigations and responses regarding application behavior, data accesses, or data changes. Application and data security controls can be installed within applications, on network or server interfaces, or alongside data files or databases.

E-Mail and Web Traffic

E-mail and web traffic security controls govern e-mail and web traffic going into and out of the organization's networks and computers. These controls are important because e-mail and web traffic are the two most common avenues for the entry of malware and the start of cyberattacks against the organization. These controls block potentially malicious messages or websites, detect potentially malicious traffic without blocking it, or support investigations and responses after a cyberattack has been detected through other means. E-mail and web-based attacks may be detected when users report unusual e-mails from unknown sources requesting their log-in credentials, or websites attempting to spoof the organization or its partners. These controls can be installed on servers, web gateways, or delivered through cloud services.

Users

User security controls can be applied to user accounts, credentials, accesses, or behaviors to ensure that people online are who they say they are. Modern networks and applications frequently serve large numbers of people identified only by their user accounts and secured by passwords or other credentials. These controls attempt to block potentially malicious user accounts or accesses, detect possibly malicious behavior for later investigation and analysis, or support investigations and responses regarding user behavior, user access to accounts (authorized or unauthorized), or account lifecycle activities (e.g., create, activate, modify, disable, delete). These controls can be integrated into user account management processes, or can be accomplished through external analytical systems.

Privileged Accounts

Privileged account security controls can facilitate the management of privileged accounts and system accounts used for systems administration within the organization's IT systems. Privileged accounts are special – and require special control treatment – because of their access to systems administration channels and system configurations. An attacker with access to privileged accounts may be able to access huge databases, turn off security protections, or even physically destroy computer equipment. These security controls restrict access to these important accounts, detect attempts to tamper with privileged accounts, or support investigation and responses regarding privileged user and system accounts. These controls can be integrated into account management processes, performed using standalone components, or installed alongside other protection technologies.

Cloud Services

Cloud service security controls protect the access, administration, and operation of cloud-based services. The controls can be delivered by the cloud provider, the cloud consumer, or a combination of the two. These controls can restrict who can do what within the cloud environment, detect attempts to tamper with the cloud environment or perform inappropriate actions, or support investigation and responses related to cyber incidents within the cloud environment. These controls can be integrated into the cloud service, delivered from the organization's own networks, or delivered through third-party cloud security providers.

Mobile Devices

Mobile device security controls can be applied to mobile devices that are entrusted by the organization for accessing its systems or processing its data. Frequently, these controls are delivered through mobile device management (MDM) technology.[1] These controls can restrict what mobile devices can do

1 *Cybersecurity* technology for managing organization data stored on mobile *devices*. This technology generally works by either controlling the device itself or by creating within the device a protected data store or container for organization data. If the device is lost or stolen, this technology usually provides the ability to erase the organization data, or even the entire device, so the data is not compromised.

with organization data, detect attempts to compromise or tamper with organization mobile devices, or support investigation and response regarding cyber threats related to mobile devices. These controls can be delivered from the organization's network or third-party providers.

Internet of Things (IoT)

IoT security controls protect non-computer devices connected to an organization's networks. These controls frequently serve to compensate for the lack of security protections built into the IoT devices themselves, or to compensate for known device vulnerabilities. These controls can restrict how IoT devices behave or communicate, detect potentially malicious IoT behaviors or communications, or support investigation and response regarding cyber attacker behavior against such devices. IoT security controls can be delivered within the devices themselves (which is uncommon), or integrated into the surrounding networks and IT systems.

Selecting Control Targets

These different cyberdefense security controls work together to provide the protections organizations need for their networks, computers, accounts, applications, and devices. Frequently, these different protections are provided by separate products and technologies, although some cyber vendors have product "suites" that combine protections against multiple cyberdefense control targets – such as endpoint protection and web filtering, or malware blocking and detection – into a single solution. When designing overall cyberdefenses, a useful way of looking at controls is to consider them in terms of prevention, detection, response, and recovery. These four types of controls are described in the next several sections.

Preventive Controls

When people think about security controls, they almost always think first about prevention. "Let's block the undesirable behavior, so it simply can't ever happen," they say. While this approach is hardly the *only* way to approach security, it is certainly an important one, and forms the foundation of many organizations' cybersecurity. Preventive controls are cheap, effective, and generally easy to validate once put in place. Some examples of common preventive controls, applied against the different control targets previously discussed, are described as follows.

Endpoint Security Prevention

Endpoint preventive controls involve (1) "hardening" endpoints to turn off unneeded functions and patch vulnerabilities and (2) tools or configurations to prevent changes to endpoints that might be malicious. Such changes might include malware installation, changes to security policies, or remote systems administration tools. Common endpoint security technologies include anti-virus and anti-malware software suites, and security configurations to block unauthorized applications or activity.

Network Security Prevention

Network preventive controls involve blocking potentially malicious network traffic from entering or transiting the organization's network. Network traffic may be blocked based on source, destination, address, port, protocol, signature, or other properties. This blocking can make it more difficult for attackers to connect to organization resources, control them remotely, or exfiltrate sensitive data. Common network security technologies include firewalls, network access control, intrusion prevention systems (IPS), and virtual private networking (VPN).

Application and Data Security Prevention

Application and data preventive controls involve blocking potentially malicious activity related to trusted applications and the data they handle. This blocking can include configuration controls to protect against unauthorized software installation, access protections, and encryption of sensitive data. Common application and data security technologies include application whitelisting,[2] file-based permissions, cryptographic key management, and data leakage protection (DLP).

---

2 Whitelisting is a security technology that monitors the specific software programs running on a computer, and only permits those that have been explicitly identified – whitelisted – to run. Applications and software programs that are not on the whitelist are not permitted to execute. Whitelisting is very effective at blocking malware, since unknown malware will not be on the whitelist. This is in contrast to anti-virus software, which only recognizes malware that has been previously recognized and placed on a list of known malicious software, or *blacklist*.

E-Mail and Web Security Prevention

E-mail and web preventive controls involve blocking potentially malicious e-mail and web traffic, usually at the organization's internet perimeter or at its endpoints. This blocking can filter out spam, malicious attachments, malvertising, and untrusted websites. Common e-mail and web security technologies include e-mail filtering, malicious domain blocking, and web proxies.

User Security Prevention

User preventive controls involve limiting access to user accounts and controlling what resources in the organization users can access. These controls are often called identity and access management (IAM). Common user security technologies include passwords, user groups, permission groups, secure provisioning, and multifactor authentication (MFA).

Privileged Account Security Prevention

Privileged account preventive controls involve limiting access to sensitive systems administration channels and account credentials. By gaining control of privileged accounts, attackers may be able to access and modify organization data at will. Common privileged account security technologies include isolated "telemetry" networks, bastion hosts, remote keyboard-video-mouse (KVM) connections, and privileged account management (PAM) credential vaults.

Cloud Security Prevention

Cloud preventive controls involve controlling access to cloud applications and infrastructures, and protecting them from abuse. Protecting cloud infrastructure can be challenging, as it is inherently internet-facing and can potentially be accessed by anyone anywhere in the world who has the right credentials. Common cloud security technologies include cloud security gateways, cloud access security brokers, and authentication federation.

Mobile Device Security Prevention

Mobile preventive controls involve controlling mobile devices used to access organization sensitive data (e.g., personally identifiable information, business information, classified information). These controls often create an encrypted partition on the device where organization data can be isolated and protected from tampering or access without credentials. Mobile device management (MDM) is the most common mobile security technology, providing access control, application control, and data encryption within a single mobile software suite.

Internet of Things (IoT) Security Prevention

IoT preventive controls involve providing protections within and around IoT devices to protect them from unauthorized access and network-based attacks. These controls can limit network access, restrict programmable logic controller (PLC) software configurations, or limit IoT network communications. Common IoT security technologies include network access control (NAC), PLC managers, and network protocol filtering.

Effective Preventive Controls

To help manage preventive controls, there are cybersecurity tool suites that include management infrastructures and consoles to design and deploy security policies across large numbers of endpoints, networks, accounts, or applications. Examples of such suites include products from Microsoft, McAfee, and Symantec. These suites often include integrated technologies for managing preventive controls, and may include monitoring and detection as well.

But what happens when prevention fails? Despite their strengths, preventive controls are not perfect. It is difficult (and expensive and time-consuming) to define preventive rules for the full range of possible scenarios. Frequently, prevention gets in the way of the flexibility and speed demanded by the business. Organizations must find "middle ground" where compromises are made between strict prevention and flexible execution. In these types of situations, detective controls may be able to "bridge the gap," as discussed in the next section.

Detective Controls

Detective controls become critically important when preventive controls fail to block malicious activities. Preventive controls cannot stop everything, and cyberattackers claim they can eventually defeat any cyberdefense. In addition, preventive controls may interfere with legitimate organization operations by blocking accounts, applications, or necessary network activity. Addressing this issue, detective controls have the advantage of allowing users to do what they want, alerting users when they do wrong, and then allowing the organization to deal with the "detected" wrong behavior after the fact. Consider the real-world analogy of law enforcement. Only a small range of potential crimes can be actively "prevented." However, law enforcement is aggressive in pursuing and punishing crimes after they actually occur or are "detected." In addition, many legitimate activities – like systems administration, software installation, network scanning, and user logins – are necessary, but potentially dangerous. In these cases, organizations require detective controls to help ensure the activities are being performed legitimately, appropriately, and safely.

Detective controls are easy and cheap to deploy, and properly deployed detective controls can effectively identify many types of malicious activities. However, these controls have the disadvantage of being "noisy," as poorly tuned detective controls can generate large numbers of alerts and "false positives." This can then generate a large number of labor-intensive investigations to make sure that everything is okay. Detective controls also require logging, correlation, and event monitoring infrastructures to catch incidents and set them up for follow-up investigation. Some examples of common detective controls, applied against the different control targets previously discussed, are described below.

Endpoint Security Detection

Endpoint detective controls involve being able to detect malicious activity occurring on endpoint computers and devices. Endpoint detective controls can also include detecting when security protections have been defeated, malware has been installed, credentials have been compromised, or other problematic activities have occurred. Common endpoint security detection technologies include malware detection and user activity monitoring.

Network Security Detection

Network detective controls involve detecting potentially malicious network traffic entering or transiting the organization's network. This detection may be based on source, destination, address, port, protocol, signature, or other properties. Because the traffic is not blocked, detection can be applied in cases where some traffic may be benign while other traffic is malicious, or in cases where defenders are not sure how blocking traffic may affect legitimate applications. Common network security detection technologies include intrusion detection systems (IDS) and network traffic monitoring and analysis.

Application and Data Security Detection

Application and data detective controls involve detecting potentially malicious activity related to trusted applications and the data they handle. Such detection can pick up where preventive controls leave off, potentially catching administrative mistakes and oversights, as well as malicious activity. Common application and data security detection technologies include file integrity monitoring, data integrity checks, and digital signatures.

E-Mail and Web Security Detection

E-mail and web detective controls involve monitoring and alerting on questionable e-mail and web behavior, without blocking them entirely. One technique is to use a secure e-mail gateway to detect and possibly block a wide variety of e-mail threats, such as malware and phishing attempts. E-mail gateways can have the capability to insert warning labels into suspicious messages to warn e-mail users, while still delivering the messages to their intended recipients. In addition, secure web gateways can show users a warning when they visit potentially dangerous websites, or download possibly dangerous content or software from the web. This type of detection is built into many e-mail filtering tools, web proxies, and internet browsers.

User Security Detection

User detective controls involve monitoring user permissions, account accesses, and account activity to detect potentially malicious activity. These controls may

use analytics and machine learning to establish activity baselines and detect deviations from those baselines. Common user security detection technologies include account authentication and activity logs, permission monitoring, and user behavior analytics.

Privileged Account Security Detection

Privileged account detective controls involve monitoring sensitive systems administration channels and account activity. These controls may use combinations of account monitoring, endpoint monitoring, and network monitoring to detect the potential abuse of privileged accounts. Such monitoring is frequently built into privileged account management tools, and may include features for logging, auditing, and recording privileged sessions.

Cloud Security Detection

Cloud detective controls involve monitoring cloud activity, applications, and data to detect potentially malicious activity within cloud environments. Cloud vendors usually provide limited detective controls through logging interfaces, but frequently it is up to the customers to design and deploy the detection they think they need. For example, customers may incorporate cloud security gateways, cloud access security brokers, and federated authentication systems into their design of cloud detection capabilities to enforce their particular security policies and detect potentially malicious behaviors.

Mobile Device Security Detection

Mobile detective controls involve monitoring mobile devices accessing organization systems and data, and detecting when those mobile devices may be compromised or malicious. Mobile device monitoring is a relatively new area of cybersecurity, as mobile operating systems are compromised far less often than traditional personal computers due, in part, to the more secure mobile operating system environment.[3] Mobile device management technologies

3 On mobile operating systems, the user does not usually have "root" or "administrator" control over the operating system, and software must run under very strict security policies. Personal

frequently provide monitoring of mobile activities, although it may also be delivered through web gateways or mobile authentication tools.

Internet of Things (IoT) Security Detection

IoT detective controls involve monitoring IoT devices to be able to detect when they have been maliciously compromised, or demonstrate behavior that is possibly dangerous to the rest of the network. Frequently, such detection is delivered through network-based controls, as IoT devices seldom have such monitoring built-in or as an installable option. Firewalls, network access control, intrusion detection systems, and other technologies can fingerprint IoT devices and may be able to detect signs of compromise.

Effective Detective Controls

Effective detection can be a game-changer for organization cybersecurity. It picks up where prevention leaves off to give the organization visibility into its IT systems and their cybersecurity behavior. Detection enables the organization to identify attackers who have defeated initial preventive controls, and potentially take action against those attackers before they achieve their objectives. Without detective controls, the organization is blind to cybersecurity failures, only finding out what happened after it appears in the headlines. *But what happens when detection succeeds?* When the organization finds out that it has an attack on its hands, it must move on to leverage the next set of cyber controls: *response controls*.

Response Controls

Response controls are activated after detection occurs. Once a detective control "fires" to alert cyber personnel of suspicious behavior, a number of follow-up actions need to be initiated. First, defenders need to *investigate* the alert to understand if the alert is a legitimate *incident*, or merely a *false positive*. Second, if

computers, on the other hand, regularly allow users to perform administrator actions that can change or defeat the operating system's protections. Consequently, it is much easier for malicious software to be accidentally installed on a personal computer than on a mobile device.

it is a false positive, defenders may want to *tune* the detective controls to improve the *fidelity* of detection and reduce *noise*. Third, if it is a legitimate incident, the defenders will want to initiate a response to *identify* the cyberattack, *contain* the attacker, and ultimately, *repel* the attack.

Cyber response is often performed from a security operations center (SOC). In the SOC, cyberdefenders may use *security orchestration* technology to integrate disparate security tools to help coordinate investigation and defense activities. Response activities may involve many individuals, including SOC personnel, IT personnel, and end users. They will all work together to figure out what happened, how it happened, and the breadth of the cyberattack in progress. A race may be on to "get ahead" of cyberattackers to stop them before they can reach their objectives. These activities then rely upon infrastructure and controls within the organization's endpoints, networks, applications, and data, to support the response process. Some examples of common response controls, applied against the different control targets previously discussed, are described as follows.

Endpoint Security Response

Endpoint response controls involve supporting the investigation and containment processes against organization-managed endpoint computers, devices, and servers. Endpoint response controls allow defenders to search through running programs, analyze network activity, and investigate user behavior. Common endpoint security response technologies include endpoint logs, forensic tools, and endpoint security monitors.

Network Security Response

Network response controls involve supporting the investigation and containment processes on organization networks and across network boundaries and perimeters. These controls enable investigators to search for network traffic related to incidents of concern, and then block network traffic they have identified to be malicious. Network security response capabilities may be provided by firewalls, intrusion detection system/intrusion prevention system (IDS/IPS), network analytics, and dedicated network response technologies.

Application and Data Security Response

Application and data response controls involve supporting the investigation and containment process within organization applications and data. They permit rapid disabling of compromised application software, or failover to "known good" backup systems. For data, they include isolation of compromised databases or files, and rollback of suspected fraudulent transactions. Frequently, these controls are delivered through configuration and change management processes, backups, data archives, and supporting systems.

E-Mail and Web Security Response

E-mail and web response controls involve enabling the containment and removal of malicious e-mail messages, attachments, web links, and websites or pages. As phishing is a common method of cyberattack, it is helpful to be able to identify phishing messages and remove them from mailboxes after they are identified but before other users can view them. Rapid e-mail response can reduce the numbers of users in the organization who open malicious e-mails, attachments, or web links. Similarly, it is helpful to be able to quickly block malicious websites or content across the entire organization, once they have been identified. E-mail and web security responses may be built into existing e-mail and web gateways, or may be performed using dedicated technologies or incident response systems.

User Security Response

User response controls involve supporting the investigation and containment process with regard to user accounts, identities, and permissions. These controls enable organizations to investigate user activity, lock user accounts, change user credentials, and analyze or reset user permissions. These controls are frequently implemented through user activity logs, enterprise directories, and identity and access management technologies.

Privileged Account Security Response

Privileged account response controls involve supporting investigations and containment of activity related to privileged systems administration channels and

accounts. These controls can include logs of privileged account activity, recordings of administrative sessions, inter-machine authentication, and the flow of data within the computer network. Frequently, these controls are implemented through privilege access management credential vaults, as well as identity and authentication infrastructures.

Cloud Security Response

Cloud response controls support being able to investigate and respond to cyber incidents within cloud environments. These capabilities require a combination of logs, application programming interfaces (APIs), account and identity management, and data forensics. Cloud response capabilities are often highly dependent on the cloud provider and the nature of the cloud service, along with the availability of logs and system redundancy.

Mobile Device Security Response

Mobile response controls enable investigations and incident responses on mobile devices. When these devices are not owned by the organization, this activity involves analyzing communications between organization IT systems and mobile devices, and tracking down data sent to, received from, or stored on mobile devices. Data leakage protection (DLP) and mobile device management (MDM) technologies provide useful capabilities and may be helpful when containment needs to extend to mobile devices.

Internet of Things (IoT) Security Response

IoT response controls support investigation and containment of malicious activity related to IoT devices. Frequently, investigations center around network activity generated from IoT devices, and analyzing network logs to understand that activity. Ideally, containment is performed by disconnecting affected devices from the network, although in mission-critical applications and manufacturing environments, this containment may not be possible or practical. Often, IoT response involves understanding the malicious behavior, and then putting in place network blocks to mitigate its potential damage until affected devices can be repaired or replaced.

Effective Response Controls

Effective response, centered around investigation and containment of malicious activity, enables an organization to catch up to cyberattacks after they start. Responses must be swift and decisive if the organization is to catch attackers "in the act" before they can reach their objectives. Logs, correlation, forensic tools, and skilled analysts are critical for timely response. Also critical is good coordination between cyber personnel and the business to manage the operational impacts of computers, accounts, and networks that may be blocked during the response process. Once the organization can respond to cyberattacks effectively, it can then move on to the final set of controls: *recovery*.

Recovery Controls

After a cyberattack or other failure has occurred and the organization has responded to it, recovery controls are engaged to close out the cyber incident and restore normal operations. Central to recovery is the concept of *restoration*, where attackers are repelled and affected computers, accounts, and networks are restored back to their status before the cyberattack occurred (without the attackers, of course). Recovery may involve restoring data and software from backups, re-provisioning accounts or credentials, resetting passwords, re-configuring networks, and strengthening cyberdefenses to address identified vulnerabilities. Recovery may also require the re-imaging or replacement of damaged IT assets such as computer drives or personal computers.

Recent developments in cyberattacks – most notably *ransomware* – have placed new emphasis on the importance of recovery as a pillar of cyberdefense. In the face of these types of destructive cyberattacks, organizations that can effectively recover and restore operations can dramatically reduce their risk. This risk reduction significantly affects the overall cost of cyberattacks even when they are successful. However, effective recovery capability requires the presence of recovery *controls* within the organization. Some examples of common recovery controls, applied against the different control targets previously discussed, are described as follows.

Endpoint Security Recovery

Endpoint recovery controls involve being able to restore endpoint computers, servers, and devices back to "known good" conditions from before attackers

compromised them or malware was installed. A major component of this control is automated backup and restore tools, although these tools may also be supplemented with known good (or "gold code") repositories of operating system and application software, system configuration logs, configuration file backups, and other resources. Backups of firmware and basic input/output system (BIOS) software may be needed to restore operation after particularly destructive malware or attacks. Recent ransomware attacks that disabled thousands of computers have prompted new emphasis on recovery capabilities. It is important for some backups to be "offline" to protect against attacks targeting backups as well as primary systems.

For a brief period in 2012, world hard drive shipments were disrupted while Saudi Aramco replaced over 40,000 hard drives to recover its IT systems from a devastating cyberattack.

Network Security Recovery

Network recovery controls involve being able to restore network infrastructures, configurations, and operations in the event of an attack. Networks are generally less of a target than endpoints and applications, but can be significantly harder to restore if their configurations are damaged. *Do you have network diagrams and backup configurations for routers, switches, and network security systems? How long would it take to recover your routing tables or firewall rules, if they were to be damaged or erased?* Network security recovery controls are frequently implemented through network configuration tools, but may also be implemented manually through configuration file backups and archives.

Application and Data Security Recovery

Application and data recovery controls can involve restoring organization applications and tools back to known-good configurations, "rolling back" databases to remove fraudulent transactions, or restoring damaged or destroyed data from backup copies. Detailed logs of application configurations, binary file backups, and source code repositories are helpful for application recovery. Data recovery hinges on transaction logs, data replication, and offline backups. When restoring operations, database and file "metadata" may be important for differentiating among legitimate and fraudulent files, records, and transactions.

E-Mail and Web Security Recovery

E-mail and web recovery controls involve rapidly restoring e-mail and web services in the event of a cyberattack. Restoring web service may be as simple as accessing the internet from the local Starbucks coffee shop, On the other hand, restoring organization e-mail systems that have been impacted by a cyberattack can be non-trivial due, in part, to multiple domains, large numbers of users, volume of actual e-mail messages, and time zones impacted. Cloud-based services like Gmail (from Google) and Microsoft's Office 365 may be helpful for rapidly restoring e-mail service, or at least for achieving limited contingency operations. Restoration should also include protections against the previously occurring cyberattack to block the attackers from coming back easily, or getting in again.

User Security Recovery

User recovery controls involve restoring compromised user accounts, permissions, credentials, and transactions. The most common user security recovery control is the well-known password reset, where users change their password to a new value unknown to the attackers who compromised the accounts. With cloud services, this password reset may be all the recovery that is possible; with internal accounts, there may be additional steps to reissue or update multifactor authentication (MFA) tokens, reset biometrics, or other measures. Heavily compromised accounts may warrant locking or deleting the original account, and generating entirely new accounts with new login credentials and permissions. Identity access management (IAM) systems and scripting may be helpful for implementing user security recovery, especially when it must be done en masse.

Privileged Account Security Recovery

Privileged account recovery controls involve resetting credentials and permissions for privileged system administration accounts and machine-to-machine system accounts. Resetting compromised system accounts can be extremely challenging, as it may require updating applications and configuration files over much of an organization. Some accounts are so "hard coded" that their passwords cannot be practically changed – in these cases, other compensating controls may be necessary. Privileged access management (PAM) and identity access management (IAM) systems may provide useful tools for performing recovery on these important accounts and restoring normal operations.

Cloud Security Recovery

Cloud recovery controls involve restoring compromised or damaged cloud applications, services, infrastructures, data, and tools. Frequently, this process also includes resetting credentials for cloud services, particularly systems administration credentials, systems administration channels, and network protections. The recovery process may also include restoring cloud service configurations, cloud-based applications, or cloud-hosted virtual machines. This recovery process may rely upon other recovery controls (endpoints, networks, applications, etc.) to restore specific aspects of the cloud environment.

Mobile Device Security Recovery

Mobile recovery controls involve restoring compromised or damaged mobile devices back to "known good" operation. This recovery may include using the "factory reset" feature of mobile device operating systems, or working with mobile providers or manufacturer support channels to reset their software and configurations. Frequently, this recovery will involve removing and re-installing organization mobile device management (MDM), applications, tools, and data onto mobile devices. Sometimes, devices may be "bricked" and unable to turn on or function, and may require manufacturer support or even physical replacement. Critical data stored on mobile devices may need to be restored from offline backups or cloud services.

Internet of Things (IoT) Security Recovery

IoT recovery controls involve restoring IoT devices affected by cyberattacks or malware back to proper operation. In many cases, it is not be possible to "repair" IoT devices that have been compromised – instead, the organization will have to weigh the pros and cons of replacing them altogether or installing other compensating controls. In other cases, IoT devices may be identified as compromised, but that compromise is not directly involved in the cyber incident. In many of these cases, the organization will simply have to make do with the devices they have, despite those devices being insecure, compromised, or otherwise vulnerable. A compromised smart refrigerator may be something that the organization can simply live with, rather than going to the trouble of trying to fix it. In other cases, the organization will be able to restore IoT firmware, do factory resets, or otherwise adjust the devices to bring them back to a secure state.

Effective Recovery Controls

In many cases, robust recovery controls can compensate for significant deficiencies in the controls for prevention, detection, and response. In addition, cybersecurity recovery controls can be coordinated with recovery controls for other contingencies such as equipment failure, supplier emergencies, personnel changes, and natural disasters. Often, a single recovery capability will be useful for a number of different recovery scenarios. Finally, devastating cyberattacks and ransomware attacks, as have occurred over the past decade in particular, show the importance of being prepared and how organizations can, in fact, recover when almost all has been lost.

Devastating cyberattacks show how important recovery is to an overall cyberdefense strategy. In 2012, Saudi Aramco had to recover more than 30,000 workstations to restore operations as the world's largest exporter of crude oil. In 2014, Sony Pictures had to restore their entire IT environment – networks, servers, computers, and data – after being wiped out by a deliberate cyberattack (most likely from North Korea). Maersk Shipping's 2017 recovery from the NotPetya ransomware was estimated to cost almost $200 million, while the City of Baltimore had to do a similar recovery from the RobinHood ransomware in 2018, at an estimated cost of $17 million.

Cybersecurity Audits and Assessments

As distinguished management consultant and author Peter Drucker famously stated, "If you can't measure it, you can't improve it." While some may argue that improvement is still possible without measurement, many would agree that if measurement can be performed, improvements are a lot easier to identify and track. Similarly, cybersecurity tends to benefit when the presence and performance of controls can be objectively evaluated and measured. This measurement may be required to meet regulatory requirements, contract obligations, or for insurance purposes. Measurement is also useful to help management choose how to allocate and prioritize limited resources to address cybersecurity concerns. This measurement of cyber controls is often described as an "audit" or "assessment." While these two words are often used interchangeably, they actually refer to very different activities:

- *Cyber control audits* are usually performed to validate compliance with an external standard, like the Payment Card Industry Digital Security Standard (PCI-DSS) or the Health Insurance Portability and Accountability Act (HIPAA). Simply stated, the output of the audit is a "yes-no" assertion of

compliance with the selected standard's requirements, along with accompanying evidence and artifacts to support that assertion.
- *Cyber control assessments*, on the other hand, are used to give management feedback on where controls are strong or weak, usually organized according to an assessment framework such the National Institute for Standards and Technologies Cyber Security Framework (NIST CSF), the International Standards Organization's ISO 27001, or a similar framework. Generally, the output of an assessment consists of observations and recommendations organized according to the framework, and intended to give management inputs on where investments should be made to improve cyberdefense controls.

Both audits and assessments can provide management with useful, actionable inputs to help improve its cybersecurity posture. Some common audit and assessment activities are described as follows.

Vulnerability Scans and Patching

Vulnerability scanning is perhaps the most common type of assessment activity, and may also be considered to be a detective control, depending on its level of automation. Vulnerability scans identify software vulnerabilities within an organization's IT systems, and help direct IT personnel to where patches may need to be deployed, or where vulnerabilities may need to be mitigated through compensating controls like network segmentation or monitoring. Organizations should be careful to ensure that identified vulnerabilities are actually mitigated, and don't become "noise" that is ignored.

Red Team Testing

This testing takes vulnerability scanning to another level by investigating whether vulnerabilities could be exploited by real-world cyberattackers to actually compromise an organization's IT environment. Red team testing can be extremely helpful, as it exposes how vulnerabilities can translate into real cyber risk. Red team testing also shows how some vulnerabilities may increase an organization's risk far more than others. A valuable use of red team testing is to verify that detective controls will be triggered by real-world cyberattacks, even if the attacks are not stopped. Organizations can use red team testing to verify how their cyberdefenses work along all of the stages of a cyberattack, using the "cyber kill chain" or "attack sequence" as a framework for analysis. Effective red team testing can be very

effective at considering how the organization's cyberdefenses will work to prevent, detect, and thwart real-world cyberattacks.

Permissions Re-Certification

A common use of an audit process is the re-certification of accounts and permissions within an organization's IT systems. Oftentimes, such re-certification is an annual process, although sponsored accounts and contractor permissions may warrant a quarterly (or even more frequent) re-certification process. The purpose of this audit process is to help the organization verify that personnel and computers have the permissions they need to do their jobs, and not more. Personnel who have left teams or roles should have those permissions removed in a timely fashion, and the same should be done for automated and service accounts that have been changed or are no longer needed. The re-certification process is often a critical component of the organization's regulatory compliance efforts, and tends to be carefully reviewed during external audits.

Regulatory Compliance Audit

Regulatory compliance audits are performed to assert compliance with external regulatory standards, like the Payment Card Industry Digital Security Standard (PCI-DSS) or the Health Insurance Portability and Accountability Act (HIPAA). Often, these audits are performed by professional auditors, following a methodology similar to that performed for financial audits or legal compliance. For each control to be audited, auditors look for *artifacts* that provide *documentation* indicating the proper *operation* of the security control. Auditors may then perform spot-checking against the control operation to find cases where the control may have missed something or been non-functional. Such cases may then turn out to be control *deficiencies*, where the control is determined to be inadequate to its task. The audit goal is to construct an *assertion* that the organization *does* or *does not* meet the requirements of the standard being audited, along with supporting evidence and documentation.

Cybersecurity Control Assessment

Cybersecurity control assessors seek to evaluate controls against their own standards of performance, and give the organization actionable feedback about where

its controls are strong, weak, or inadequate. Assessment results are seldom binary "yes or no" determinations – rather, they tend to be graded on scales from 1 to 10, or on maturity levels ranging from 1 to 5, or something along those lines. Sometimes, assessment results may not be quantitative at all, and may instead consist simply of observations and recommendations for improvements. It depends on the assessors, the assessment methodology, the framework being used for the assessment, and the goals of the organization's cyber management.

Deficiency Tracking and Remediation

In the cases of both audits and assessments, an organization will likely end up with a "to do list" of improvements that are either mandatory for compliance or encouraged for improvement. These improvements should be formally tracked. In many cases, regulatory compliance requires the improvements to be not only tracked but also remediated prior to the next subsequent audit. Continued control deficiencies may lead auditors to determine that a control is "not effective" and discount its value in achieving regulatory compliance. Even when tracking is not required for compliance, it can be helpful to keep an organization's staff focused on implementing improvements, even while juggling other priorities.

Aligning Cyber Controls

In these cases, cyber control audits and cyber control assessments can be just as important as the actual control implementation and operation. When an organization has controls that do not need to be audited or assessed on a regular basis, one may want to ask: *Are such controls really necessary, or are they merely "nice to have" uses of resources that could be better used elsewhere?* The goal of these efforts is to help an organization stay focused on aligning its cyberdefenses with the business risk mitigation effort. Cybersecurity capabilities should reduce the business' risk, whether that risk be related to compliance, competition, operation, customer delivery, or data protection.

Cybersecurity Technologies and Capabilities

Cybersecurity technologies and capabilities enable the automation of the organization's cyberdefenses, and are used to implement preventive, detective,

response, and recovery cyber controls. A single technology may provide multiple capabilities, and support multiple controls simultaneously. For example, a network firewall can both block an attacker's network traffic and also raise an alert that an attack has just occurred. Cybersecurity technologies can be very powerful because once they are deployed, they tend to "just work." However, to live up to this potential, cybersecurity technology solutions need to be carefully engineered, regularly maintained, and constantly monitored.

Cyberdefense technologies and capabilities are discussed in greater detail in a later chapter of this book.[4] Some examples of how cyberdefense technologies can be used in practice are as follows.

- *Using Multifactor Authentication (MFA)* for internal systems administration, as well as remote access to the organization's sensitive systems.
- *Using Bastion Hosts* to isolate systems administration channels and perform access control on systems administration functions.
- *Deploying Command Logging and Analytics* to analyze systems administration activities and detect administrator credential abuse.
- *Deploying Log Aggregation* to create a single audit trail for the organization's cyber systems, and to enable log correlation and analysis.
- *Using Data Encryption and Tokenization* to protect sensitive data stored in databases, backup files, or non-production systems.
- *Deploying Database Firewalls* to isolate application databases from internet-facing application servers and control systems administration access.
- *Using Data Leakage Protection (DLP)* to detect attempts to transfer sensitive data outside of the organization's network and access-controlled systems.
- *Using Forensic Imaging* to support investigations of cyber incidents, by taking "snapshots" of compromised system memory and storage.
- *Using Mobile Device Management (MDM)* to manage mobile devices accessing the organization's e-mail, calendar, and intranet services.

Cybersecurity Operational Processes

Cybersecurity operational processes enable the organization to operate its preventive, detective, response, and recovery cyber controls. While technologies may automate control operations, people are necessary to design, deploy, maintain, and monitor those technologies. People need to take action when the cyber technologies indicate malicious activities are occurring. The work people perform to

4 See Chapter 7, "Cybersecurity Capabilities," for a detailed discussion of cybersecurity capabilities and the technologies that enable them.

maintain the organization's cyberdefenses can be described and organized in terms of operational processes.

Cyberdefense operational processes are discussed in greater detail in a later chapter of this book.[5] Some examples of how operational processes can be used to protect the organization are as follows.

- *Updating Firewall Rules and Network Filters* to block potentially malicious network traffic and reduce the organization's network attack surface.
- *Re-Certifying Accounts and Accesses* so that accounts and access permissions that are no longer needed can be removed in a timely fashion.
- *Performing Routine Patching* to update systems with the latest software code and remediate software vulnerabilities or security gaps.
- *Testing Detection Systems* to verify that detective controls can alert on potentially malicious activity to catch real-world cyberattacks.
- *Investigating Potential Incidents* to filter out false positives, investigate potential cyberattacks, and initiate containment, remediation, and recovery.
- *Recovering Lost or Corrupted Data* to recover from the damage caused by cyberattacks, compromised applications, or re-imaging of computer systems.

5 See Chapter 8, "Cybersecurity Operations," for a detailed discussion of cybersecurity operational processes and the activities they include.

Chapter 5
Cybersecurity Drivers

Why do we perform cybersecurity? To reduce risk, of course! *But what risks are we seeking to reduce? Cyber risks? Business risks related to IT systems? Risk of regulatory actions or lawsuits?* Risk comes in many forms, particularly in the presence of complicated operating environments. In addition to risk, organizations are frequently subjected to requirements and obligations stemming from external sources, such as contracts, standards, or government regulations. Frequently, this compliance must be verified through audits and assessments (internal or external) or some form of attestation or declaration of compliance. As depicted in Figure 5.1, this chapter considers some of the *cybersecurity drivers* impacting an organization's cybersecurity efforts.

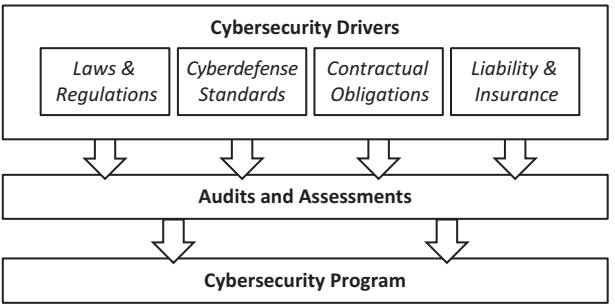


Figure 5.1: Cybersecurity drivers are verified through audits and assessments and impact an organization's cybersecurity program.

Cybersecurity drivers require organizations to take certain measures within their cybersecurity programs to ensure those programs remain compliant with the drivers' requirements. This chapter describes the following drivers: (1) laws and regulations, (2) cyberdefense standards, (3) contractual obligations, and (4) liability and insurance. This chapter considers how organizations can manage to balance these cybersecurity drivers with considerations of cost and complexity, while also striving to "do the right thing" for their employees, partners, and customers.

https://doi.org/10.1515/9781501506529-005

Laws and Regulations

Many laws and regulations have been created around the world to address cybersecurity concerns. Moreover, because of the global nature of internet access, many of these laws have wide-ranging scopes in practice. For example, a business may become subject to the EU General Data Protection Regulation (GDPR) regulation if the business has a single customer who is an EU citizen, even if the rest of its corporate operation is located in a different country. Some influential cyber laws of the past two decades are described as follows.

General Data Protection Regulation (GDPR)

Passed in 2018 by the EU, GDPR is a wide-reaching regulation governing the protection and processing of personal data regarding EU citizens and businesses. It consists of 11 chapters of requirements, organized into 99 articles and 173 recitals. Noteworthy to GDPR is the "Forget-me" clause that requires organizations to be able to, upon request, completely delete an EU citizen from their IT systems. Due to the global nature of IT, GDPR is causing many organizations worldwide to upgrade their IT systems to support GDPR and to deliver GDPR-compliant privacy services to many or all of their global customers.

Sarbanes-Oxley (SOX)

Passed in 2002 by the US and commonly referred to as "Sarbox" or simply "SOX," this law seeks to increase the visibility and accountability regarding corporate financial tracking and reporting. In doing so, the law places considerable requirements on public company financial systems, their supporting IT infrastructures, and the security controls protecting them. It also places personal criminal liability onto company officers regarding financial reports and reporting. As a consequence, many US public companies consider their SOX controls to be among their most important compliance requirements.

Gramm-Leach-Bliley Act

Passed in 1999 by the US, this important piece of financial legislation repealed parts of the Glass-Siegel Act, originally passed after the Great Depression. The Gramm-Leach-Bliley Act removed barriers to consolidation among financial

institutions, allowing the merger of Citicorp with Traveler's Insurance. It also emplaced additional requirements on financial firms regarding the handling and sharing of personal information, driving many of the policies governing how these organizations process consumer financial data.

New York Cyber Security Regulation

Passed in 2017 by the US state of New York, this state-level law placed specific cybersecurity requirements on financial institutions operating within New York. Due to the significance of New York – particularly New York City and Wall Street – in the US financial industry, this law has had significant impact on both the US financial industry and the international financial industry. The regulation places specific requirements on the cybersecurity of financial institutions, including cybersecurity for third-party providers and the use of multifactor authentication (MFA).

Federal Information Security Management Act (FISMA)

Passed in 2002 by the US government and subsequently updated in 2014 (FISMA 2014), this act requires US federal agencies to emplace cybersecurity protections on their information systems. It also directs the National Institute for Standards and Technology (NIST) to create open standards and other guidance for performing and measuring cybersecurity effectiveness. As a consequence of this legislation, cybersecurity for US federal information systems is performed and measured according to defined standards published by NIST.

Health Insurance Portability and Accountability Act (HIPAA)

Passed in 1996 by the US, this important piece of legislation established requirements for the identification and protection of personal health information (PHI). By requiring certain protections for health information stored "in electronic form," it effectively requires cybersecurity controls around healthcare IT and electronic health records (EHRs).

Evolving Laws and Regulations

Laws, regulations, and standards all work together to establish clear and measurable requirements for cyberdefense performance. However, cybersecurity performance is still a new field, and cyberdefenses struggle to keep up with ever-changing IT systems that include myriad clients, servers, mobile devices, and cloud computing. Laws cannot possibly be passed or amended quickly enough to keep up with IT innovation as it is occurring. Compared to laws, regulations and standards can be more agile and more responsive to the governance needs of the latest technologies.

Cyberdefense Standards

To help organizations and regulators organize their efforts to perform and measure cybersecurity, many cybersecurity standards have been developed. Some of these standards come from formal regulatory bodies, like the US National Institute for Standards and Technology (NIST) or the Federal Financial Institutions Examination Council (FFIEC). Other standards come from industry associations like the International Organization for Standardization (ISO) or the Payment Card Industry (PCI).

Cybersecurity standards are frequently written as sets of requirements or controls regarding organization cyberdefenses. Standards might require organizations to have network firewall protections around their servers, or employees to review security logs to identify cyberattacker activity. These requirements – there can be hundreds of requirements per standard – may then be organized into groups or categories for easy management. This grouping helps to organize cybersecurity planning and assessment. The grouping may also be used for "scoring" organizations' performance against the standards. Standards may include evaluation criteria used for scoring, or scoring may be reliant upon the expertise of the assessor or auditor. Some of the more commonly used cybersecurity standards are described in the following sections.

International Organization for Standardization (ISO) 27001

The ISO 27000 series of standards for cybersecurity were first published in 2005, based on the British Standards Institution (BSI) Group's 7799 standards work. The ISO 27000 series was substantially revised in 2013. The 2013 revision includes 114 controls organized into 35 control groups and 14 clauses for

cybersecurity management. A major theme of the ISO standard is management oversight for cybersecurity controls and performance. A second major theme is accountability: *Does the organization actually perform the cybersecurity controls that it claims to have*? The ISO framework includes a comprehensive method for assessing security risks, considering controls to mitigate those risks, and an "overarching management process" to oversee the risk management and mitigating controls on an ongoing basis.

Center for Internet Security (CIS) Top 20 Critical Controls

This framework evolved from the SANS[1] Institute's 20 Critical Controls, first developed in 2008 and published in 2011. Central to this framework is its structure of 20 IT controls that are intended to be simpler to understand than other frameworks, which might contain hundreds of requirements to consider. In Version 7, the framework categorizes the 20 controls as "Basic," "Foundational," or "Organizational," and defines 171 sub-controls within the 20 controls. This framework enjoys wide industry support due, in part, to its specificity and actionality. SANS and CIS have also been quick to update and revise the controls to account for new cybersecurity techniques and technologies, and to address emerging cybersecurity threats and risk areas.

Statement on Standards for Attestation Engagements #16 (SSAE 16)

This framework was formerly published as the Statement on Auditing Standards #70 (a.k.a. SAS 70) and is frequently used by auditors to measure and report on the state of IT cybersecurity controls. This framework is frequently used for showing compliance with SOX or other legal requirements. The "SOC 1" report format shows the state of the audited organizations' controls at a given moment in time, while the "SOC 2" report format shows the status of those controls over a minimum 6-month period. The SOC 2 report is often used by software-as-a-service (SaaS) providers and cloud service providers to demonstrate cybersecurity compliance to their customers, or to satisfy customer-specific contract cybersecurity requirements.

---

1 SANS stands for "SysAdmin, Audit, Network, Security" indicating security practice areas of interest to its founders back in 1989. The organization has since become a leading global provider of cybersecurity training. Today, the acronym SANS, like the company name RSA, is almost never actually spelled out.

NIST Cyber Security Framework (CSF)

The NIST CSF was published in 2014 to respond to a presidential directive that NIST establish an open standard for conducting cybersecurity across American government and industry. The framework was unusual at the time for aligning cybersecurity practices with the incident response process's five cybersecurity functions: "Identify," "Protect," "Detect," "Respond," and "Recover." The framework does not specify specific cybersecurity controls, instead organizing the breadth of organizational cybersecurity into 23 categories and 108 sub-categories for discussion and implementation (version 1.1). The framework has been widely adopted for assessment and reporting on cybersecurity programs to business leaders and boards of directors, particularly in the United States.

NIST Special Publication (SP) 800-53

NIST special publications provide guidance on particular areas of IT and cybersecurity, primarily focused on the US government and supporting industry. SP 800–53 is a control catalog for use by US federal information systems under the NIST Risk Management Framework (RMF).[2] The RMF includes steps for assessing the criticality of information systems, with a criticality rating determining which controls are in-scope and required to be implemented. The Revision 4 framework contains 224 controls, grouped into 18 families. This framework is widely adopted in the US federal government for its information systems, its contractors, and its cloud service providers. While the published version of this framework can be overwhelming – the framework and assessment guide are over 1,000 pages long combined – this framework has the advantage of being painstakingly thorough, well-documented, and straightforward to assess.

Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool (CAT)

The FFIEC is a US banking regulatory body "empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions." FFIEC developed CAT to address the question of cybersecurity

2 The Risk Management Framework is documented in another NIST special publication, SP800-37.

standards for the financial industry, enable organizations to self-assess their risk and their risk posture, and facilitate cybersecurity awareness among financial institutions. The CAT consists of three major sections: (1) an assessment of "inherent risk" based on organization size and scope; (2) a "maturity assessment" based on the presence or absence of required controls; and (3) practical Intelligence-led Cyber Attack Simulation Testing (iCAST). The 2017 maturity assessment framework involves evaluation against 494 declarative statements that are grouped into 34 components, 15 assessment factors, and 5 domains. For assessment or audit, specific declarative statements are selected based upon the organization's inherent risk profile, with more declarative statements applied to higher-risk organizations.

Payment Card Industry Digital Security Standard (PCI-DSS)

The payment card industry has been heavily affected by cybersecurity breaches, as hundreds of millions of credit cards have been compromised in breaches at companies including Target, Home Depot, Cardsystems Solutions, Global Payments, and many others. As a consequence, the payment card industry pays great attention to its standards for digital security of payment card data, while also investing in new technology like chip-based smart cards from the Europay Mastercard Visa (EMV) consortium. Organizations that process payment card transactions (generally credit and debit cards), are subject to the 12 requirements of the PCI-DSS standard, covering protection of networks, databases, applications, and other IT systems. PCI-DSS requires organizations to have their compliance tested periodically by external, independent assessors. There are four levels of compliance to be considered, based upon the number, type, and value of the transactions processed each year.

Health Information Trust (HITRUST) Alliance

To help medical institutions comply with the cybersecurity requirements of HIPAA and other regulations, the HITRUST Alliance was created in 2007. This organization maintains the Common Security Framework (CSF) and other tools, along with education programs for medical organizations protecting sensitive medical information. The HITRUST Alliance is led by a board of directors selected from medical organizations, medical technology developers, and electronic health record (EHR) providers. The HITRUST Alliance promotes assessment and compliance with its CSF as a method for measuring and managing healthcare cybersecurity risk.

North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)

Similar to FFIEC for the financial industry and the HITRUST Alliance for the medical industry, the nuclear energy industry in the US, Canada, and Mexico has its own framework for cybersecurity. This framework focuses on controls surrounding IT systems of the "Bulk Electric System (BES)" with the IT systems identified as having "high," "medium," or "low" criticality levels. As of Version 5, this framework contains 32 cybersecurity requirements, grouped into 10 areas, labeled "CIP-002" through "CIP-011." Like the other frameworks, NERC CIP is designed to help energy producers manage their cybersecurity, and also for independent auditors to verify the management of that cybersecurity against the standards of the framework.

Varying Cyberdefense Standards

As demonstrated by the variety of the cybersecurity standards above, they are hardly "one-size" fits all, and demonstrated compliance with one set of standards is no guarantee of compliance with another set of standards. In fact, even the definition of "compliance" varies from standard to standard. Cybersecurity standards are still relatively new, and there is still a lot of room for improvement, standardization, and consistency. In addition, cyber standards are hardly the only set of requirements to consider. Specific contracts and business arrangements may contain additional cyber obligations for the organization to consider.

Contractual Obligations

Contractual obligations are usually the most explicit cybersecurity requirements for organizations, but they can also be some of the most ambiguous. Contractual obligations are explicit because they come from a specific agreement to perform a specific task regarding specific sets of data. On the other hand, contractual obligations can also be ambiguous due to unclear specifications of affected IT systems, inexact scope or time period, weak definitions, or imprecise language. Contract drafters frequently do not have the advantages of industry panels, committees of experts, or lengthy review periods to help them clearly define cybersecurity requirements.

Contract terms frequently cite cybersecurity requirements and may even attempt to tie contract consequences to cybersecurity lapses or deficiencies.

Contracts may reference cybersecurity by citing industry standards, or by defining specific cybersecurity requirements. These requirements and standards may then be applied to customers, third parties, or business transactions. Contracts may include combinations of multiple cybersecurity factors, with implied regulatory requirements alongside specific "asks." Some of the ways that contractual obligations may refer to cybersecurity are described as follows.

Industry Standards

Contracts may require adherence to specific industry standards as a requirement for contract compliance. For example, organizations processing credit card transactions are required by their card processing agreements to comply with elements of the PCI-DSS standard. In addition, contracts may require audit or attestation of compliance to cybersecurity standards like the SSAE-16 standard. In addition, contracts may require the provider operate in accordance with "applicable regulations" – for example, a data processor organization handling data that is covered under HIPAA or GDPR. Due to the nature of the work being performed and the data being handled, the contract is subject to applicable standards and regulations.

Customer Contracts

Customer contracts may include specific cybersecurity requirements having to do with the nature of the data being handled, the processing being performed, or the results of the analysis. Customers who are sharing their proprietary data with their contractors will likely include specific cybersecurity requirements regarding the handling of that data. An example of this requirement is customer proprietary data that may have to be handled on the customer's IT systems or within the customer's facilities, and never taken offsite. The customer may require its proprietary data be securely deleted after it is processed, or not retained after the termination of the contract. The customer may also require security controls – such as anti-virus, network protection, or multifactor authentication – around IT systems handling their data.

Third Party Contracts

As IT has gotten more complex and cybersecurity has become more of a business issue, organizations have given greater attention to third-party relationships and the contracts that facilitate them. It is not uncommon for organizations to require due diligence of their third parties prior to contract award, and then periodically thereafter. This due diligence might include specific cybersecurity requirements, compliance attestations, or even active testing and validation of cybersecurity protections. Many organizations engage cybersecurity services to test and score their third-party suppliers' cybersecurity, and may question the viability of suppliers who score poorly on these tests.

Partnerships, Mergers, Acquisitions, and Divestitures

Few business activities are as sensitive as business transactions, including partnerships, mergers, acquisitions, and divestitures. In each of these cases, businesses seek to securely share certain data and information, while keeping other data and information isolated and proprietary. The contracts specifying these relationships frequently identify personnel, organizations, locations, finances, and information to be shared, while also identifying others that are to be kept isolated. IT and cybersecurity must work closely together to establish preventive and detective controls to facilitate the needed sharing and collaboration, while protecting against potential "leakage" or "over-sharing." Cybersecurity failures can have significant ramifications, including damaging morale, losing key personnel, leaking proprietary information, or even jeopardizing the entire business relationship or transaction.

Interpreting Contractual Obligations

In these examples, contracts will be drafted to attempt to capture in writing the most important factors, and the areas of greatest concern regarding the contract's information security requirements. However, what is captured in the contract will seldom be complete. It will then be up to IT and cybersecurity personnel to "read between the lines" and interpret the contract language into specific technical requirements that can be implemented cost-effectively using the available technology. Cybersecurity personnel should document this interpretation so they can defend their decisions, should there be problems later.

Liability and Insurance

While regulations and specific contractual requirements cover a great deal of real-world cybersecurity requirements, these cybersecurity drivers are hardly the only sources of cyberdefense obligations. Liability is also a significant concern, particularly in the litigious United States. When consumer data is involved, organizations suffering breaches may be subject to litigation from consumer groups, even before they are subjected to regulatory scrutiny. One of the interesting factors involved in the 2017 Equifax breach[3] is that while Equifax was in possession of data belonging to hundreds of millions of people, it did not actually have direct business relationships with most of those people. This lack of a business relationship made it hard to establish which laws might have been broken or what financial damage might have occurred to the victims. While millions of consumers were affected by the breach, they actually had little legal recourse to recoup damages against Equifax.

Demonstration of "damages" continues to be a challenge, especially where personal data is involved. Although having your personal identifiable information (PII) or your protected health information (PHI) leaked to the public is bad, it is difficult to attach a specific monetary number to the damage caused by the leak. Regulators, industry professionals, and lawyers are continually trying to determine damages. Newer laws and regulations like GDPR attempt to address this challenge by specifying penalties for organizations that suffer breaches, even if actual monetary damages cannot be proven. All of these factors make calculating liability – and insuring against that liability – very difficult in the cyber arena. For organizations with potential cybersecurity liabilities, some of the key areas to consider are described as follows.

Demonstrating Due Diligence

Organizations can be prepared to defend themselves by first demonstrating "due diligence." This preparation involves having cybersecurity controls that are in line with industry norms, and collecting from those cybersecurity controls artifacts and other evidence that demonstrates the controls are in place

3 The 2017 Equifax breach lasted approximately 2.5 months and exposed the personal information (e.g., social security numbers, birth dates, addresses, driver's license numbers) of 143 million American consumers, along with similar information from people in the United Kingdom and Canada. Https://www.consumer.ftc.gov, US Federal Trade Commission Blog, September 8, 2018.

and functioning properly. The organization should also have documentation indicating its cybersecurity plans, its identification and treatment of cybersecurity risks, and its consideration of cybersecurity threats. These documents, e-mails, and other artifacts provide evidence that the organization is taking cybersecurity seriously and is doing due diligence in line with industry norms.

Defending Against Negligence

By demonstrating due diligence and serious treatment of cybersecurity considerations, organizations can defend accusations of negligence should things go wrong. However, bear in mind that prosecuting lawyers will try to seize on every mistake to argue that the organization was negligent in its cybersecurity responsibilities. Defenses against negligence will frequently revolve around showing that cyber practices were in line with industry norms, and that the overall cybersecurity program was managed according to an overall strategy and framework driven by known risks and threats. Having written documentation of these types of cyber practices can be a critical component of an organization's legal defense.

Insurance Requirements

Litigation has led to dramatic increases in the use of cyber insurance, and the consideration of cyber incidents within existing business insurance coverage. As the number of cyber incidents cases resulting in insurance payouts have increased, insurers have become increasingly specific in their due diligence and their requirements for cybersecurity protections. Consequently, this trend has resulted in increased work for everyone. One factor to keep in mind is that insurance requirements are proprietary and may evolve faster than published standards, regulations, or laws. Organizations should review their insurance coverage regularly and ensure their cyberdefenses are in line with their insurers' expectations and requirements.

Managing Liability and Insurance

Liability, due diligence, negligence, and cybersecurity insurance continue to be significant drivers for organizational cyberdefenses. The fear of cyber litigation has become more real for organizations in the wake of high-profile breaches

like Anthem healthcare (which impacted approximately 79 million people) and expensive cyber incidents like Maersk Shipping ($200 million recovery). These breaches and the litigation surrounding them have led to increased attention in this area on the part of organizations, insurers, and their attorneys, alike.

Doing the Right Thing

Implementing a successful real-world cybersecurity program involves balancing cybersecurity drivers with the rest of the organization's business priorities. Often in cybersecurity, the organization leadership knows what *should be* done, but the resources to *do it* are insufficient. Therefore, the organization must prioritize its cybersecurity efforts to deploy an incomplete solution that is effective, even though it may not be as comprehensive as desired. The challenge is how to allocate scarce resources so that the organization's overall cybersecurity can be successful as possible.

Organizational leaders may want to "do the right thing," but defining "right" is difficult and unclear. In the absence of a clear definition, organization leaders must try to understand what cybersecurity drivers apply to their IT and cybersecurity systems. Cybersecurity drivers might include protecting customer privacy, partner data, or the organization's own intellectual property. Once the drivers are identified, cyber leaders can design a cybersecurity program that can be defended as meeting the requirements, while also being efficient and economical. Balancing cybersecurity drivers with the rest of the organization's business priorities involves iteratively assessing cyber risks, prioritizing them, and then resourcing and executing progressive improvements to the organization's cybersecurity program.

Some security professionals have joked, "Compliance does not equal security." Organizations must be aware that cybersecurity success requires more than completing a series of audits and achieving a barely passing score on each. Since there are limited organizational resources, tough resource allocation decisions will have to be made. Organizations can achieve cyberdefenses that are successful, while also being economical, by considering a number of factors such as those described in the following sections.

Defining Scope

By defining scope, organizations can limit their cybersecurity focus to where it really counts. If the organization's main cyber liability is associated with credit

card processing, then the organization can limit its liability by isolating credit card processing systems and focusing its cyberdefenses around just those systems. If the organization's main liability is in its datacenter, then it can limit its liability by isolating the datacenter and strongly controlling its access and operations. By defining a narrow scope and then isolating and protecting the IT systems that are within that scope, organizations may be able to reduce the costs of managing their cyber risks.

Achieving Visibility

Complexity is an increasing challenge as IT systems increase in size, number, capability, and sophistication. Within defined cybersecurity scopes, organizations must strive to achieve visibility of the IT systems, the users of those systems, the software on those systems, and the data that the systems process. Organizations must also consider their supply chain and external connections used for processing data outside the organization. In many cases, automation may be required to maintain this visibility, as networks, devices, and configurations are constantly changing.

Defense in Depth

Once visibility is achieved, organizations must strive to protect sensitive data and systems with multiple layers of security controls. This security approach is commonly called "defense in depth," and its goal is to ensure that if one security control fails or is disabled, attackers will still have to defeat one or more additional, supplemental security controls before they can achieve their objectives. By having at least two security controls working together to stop attackers, defenders give themselves room for individual protections to have flaws or malfunctions before disaster occurs.

Detection and Response

The defense-in-depth approach cannot be fully successful if it is not paired with the *detection* of security controls that have been disabled or defeated. Detection is necessary to give defenders an opportunity to implement a *response* after the attack has started, but before damage can be done. By having detection capabilities that are triggered after the initial failure, organizations

may be able to reduce their costs for cyber protections, by using less-expensive technologies and avoiding best-of-breed, high-cost premium products. Two open-source technologies that are 90% effective each, may be just as good as a best-of-breed capability that is 99% effective, while being cheaper to procure. This redundancy can then result in reduced labor costs for investigating and responding to cyber incidents, thanks to a more-robust defense.

Striving for "Good Enough" Cybersecurity

By containing cyber scope, achieving visibility within the scope, using defense in depth, and having detection and response capabilities, an organization can strive to achieve cybersecurity that is "good enough" without being prohibitively expensive. The overall challenge is to spend the available budget on the "right" cybersecurity capabilities to impede real-world attacks, while still complying with the organization's cyber obligations and requirements.

Chapter 6
Cyber Program Management

Once an organization understands its cybersecurity business drivers – laws and regulations, cyberdefense standards, contractual obligations, liability and insurance – it can look into how to put in place an effective and enduring cybersecurity program to accomplish its security goals. As enticing as it might be to immediately start implementing technologies like firewalls or identity management, it is important for an organization to realize that most cybersecurity failures start with people, first.

The No. 1 weak link for businesses when it comes to cyber security – by a long, long way – is the people who work in the business.[1]

Consequently, an organization needs a cyber program management approach to oversee a comprehensive portfolio of cyber projects involving *technology*, *processes*, and *people*. Such projects should be aligned with the organization's overall business goals and operating environment to be effective. By putting in place a well-defined cybersecurity program with clear lines of policy and authority, the organization can get the budget that is needed, apply that budget effectively, and have visibility into its cyber status and progress over time. Figure 6.1 depicts the major cyber program management elements described in this chapter.

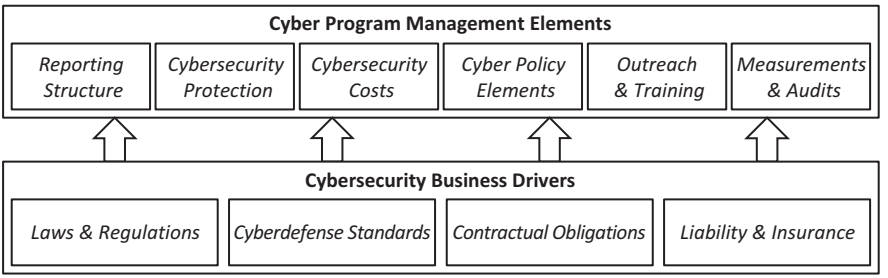


Figure 6.1: An *effective* cybersecurity program considers multiple management elements to satisfy the organization's cybersecurity business drivers.

1 Symantec, "You Are the Weakest Link: 5 of the Biggest Cyber Security Risks for Businesses," December 6, 2017.

https://doi.org/10.1515/9781501506529-006

This chapter describes reporting structures that an organization may implement for managing its cybersecurity, along with associated challenges. The chapter describes how cybersecurity protection can be balanced with other business imperatives. The chapter considers different techniques for managing cybersecurity costs. The chapter then presents the elements of a cybersecurity policy and ways in which an organization can document and deliver such elements. The chapter describes representative high-level outreach and training program activities to facilitate organizational cyber awareness. Finally, the chapter considers how measurement and audits can be used to monitor and report on cybersecurity program status and performance over time.

Determining Cybersecurity Program Reporting Structure

An important cybersecurity program consideration is determining where to place the program within the organization's hierarchy. Program placement establishes its level of authority with respect to other parts of the organization, how and where it gets its funding, and how much priority it receives "when the chips are down" and when tough business decisions need to be made. When budgets are tight, deadlines are pressing, or customers are complaining, cybersecurity needs to be able to defend itself against potential inclinations to reduce cyber priorities or budget. Cybersecurity needs to guard against such compromises by clearly articulating the rationale for the cyber protections to the management reporting structure, along with how cybersecurity enables organizational goals and corresponding business benefits.

There is no "one right way" to organize cybersecurity within an organizational structure. Each reporting structure reflects different sets of organizational tradeoffs, making certain activities easier and more efficient, while making other activities harder and less efficient. Some of the more common cybersecurity reporting structures, and their inherent tradeoffs, are described as follows.

Cybersecurity under Compliance

In this reporting structure, cybersecurity is organized underneath the compliance or legal department, frequently reporting up to a chief compliance officer (CCO) or equivalent. When organized this way, cybersecurity has strong alignment with the organization's compliance requirements, and should be closely coordinated with internal and external auditors. The challenge of this organization

structure involves the "ivory tower stigma," where cybersecurity becomes isolated from the daily business and IT activities. As a result, it becomes difficult for cybersecurity to work collaboratively with IT and the business to negotiate potential security tradeoffs, develop new product or service offerings, and identify previously unknown issues.

Cybersecurity under the Chief Information Officer (CIO)

In this reporting structure, cybersecurity is organized underneath the chief information officer (CIO), frequently with a dotted line to legal or compliance outside the CIO's organization. The strength of this reporting structure is better coordination of cybersecurity with the rest of IT, along with improved communication channels between cybersecurity and the rest of the business. The challenge of this structure is that when cybersecurity issues escalate, it is very tempting for the CIO to simply overrule cybersecurity in favor of IT operational imperatives.

Cybersecurity under Product or Service

In this reporting structure, cybersecurity is organized underneath a product or service offering, or within business operations, perhaps under the chief operating officer (COO). The strength of this reporting structure is a good alignment of cybersecurity with product or service offerings, and this approach can be very useful when the organization's cybersecurity directly affects the security posture of its clients and their data. The challenge of this structure is that cybersecurity may adopt a "one-size-fits-all" approach based on the security requirements of a single customer or a group of customers. The organization may find that it struggles to address differing cybersecurity requirements from other customers or other areas of the business.

Cybersecurity in Charge

In this reporting structure, cybersecurity is organized as a principal function, usually with IT or product development subordinated underneath the chief information security officer (CISO). While this organization may be adopted for primarily symbolic or public relation purposes, its strength is that it elevates cybersecurity to a role of paramount business importance. This strength is true

even when such security results in increased costs, reduced agility, or other business tradeoffs. This reporting structure is most useful when a cyber failure can have catastrophic consequences for the organization or its clients, and a relatively uncompromising cybersecurity approach is warranted.

Cybersecurity for Cloud and "Development and Operations" (DevOps)

While not a reporting structure per se, cloud-first environments using DevOps methodology[2] require special consideration. When an organization performs cloud-based DevOps, whether it is in a private cloud or a public cloud, the organization's entire IT infrastructure becomes represented as code. This code can include *configuration code* for networks, servers, tools, data schema, and system interconnections, along with *software code* for tools, programs, and applications. When an organization uses DevOps and cloud environments, cybersecurity must closely monitor DevOps activity to make sure the systems and applications are being built and operated in a secure fashion. This reporting structure frequently requires cybersecurity to be significantly more *tightly integrated* into the DevOps application development and deployment process than in a traditional data center environment. This integration is sometimes called DevSecOps.[3]

Cybersecurity Team Sub-Functions

Once cybersecurity's overall position in the organizational hierarchy is established, cybersecurity can continue to consider how to organize its department. Once again, there is "no one right way" to organize a cybersecurity department. Some departments will have more sub-functions and teams, while other departments may collapse multiple functions together into single teams. Figure 6.2

2 DevOps is a software engineering practice that integrates development (e.g., software developers) and operations (e.g., IT infrastructure engineers) professionals into teams to achieve rapid development cycles that frequently and reliably deliver software products, features, and services to customers. DevOps typically requires an integrated set of software tools designed to coordinate an automated release process throughout the entire software development life cycle (e.g., requirements, design, development, testing, deployment, operate, retirement).

3 DevSecOps – Similar to DevOps with respect to rapid development cycles, frequent and reliable software applications to customers, along with security "built into" applications rather than "bolted on" after the applications are released. DevSecOps promotes a philosophy that security is everyone's responsibility, versus a centralized security decision-making authority.

shows some of the major sub-functions and teams that could be a part of the cybersecurity department.

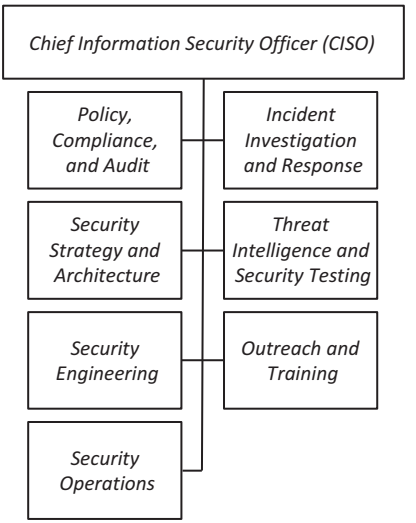


Figure 6.2: This notional CISO organization depicts potential cybersecurity sub-functions and teams.

These major cybersecurity department sub-functions can be described as follows.

Policy, Compliance, and Audit

This team is responsible for establishing cybersecurity policy and standards, coordinating compliance with applicable regulations and external standards, and conducting audits to verify compliance. This team frequently has a close relationship with corporate compliance or legal departments, and may also be involved in handling the regulatory impact of cybersecurity incidents.

Security Strategy and Architecture

This team is responsible for defining the organization's overall security strategy, priorities, and control framework. It also considers the overall architecture of how cybersecurity capabilities and services will fit together to deliver the cybersecurity controls needed by the organization. It may also select the preferred suppliers for those capabilities and services.

Security Engineering

This team is responsible for designing and implementing cybersecurity controls within the organization's IT systems. It may also work with other departments, like IT or application development, to ensure that security is "baked in" to IT systems and software applications. This team oversees major design changes and enhancements to operational cybersecurity systems.

Security Operations

This team is responsible for operating the organization's cybersecurity controls and technologies on an ongoing basis. This responsibility should include the operation of preventive and detective control systems, investigation of detective control alerts, and reviews of application and system event log files. This team may also be responsible for maintaining and patching security infrastructure systems, once the systems are operational.

Incident Investigation and Response

This team is responsible for investigating cyber incidents identified by IT operations, and then performing or coordinating appropriate incident responses. An incident response would include investigation, triage, containment, and remediation of compromised systems, networks, or accounts. This team might work with other cyber teams or IT departments to determine the regulatory impacts of cyber incidents that occur.

Threat Intelligence and Security Testing

This team is responsible for staying aware of cyber threats and testing the organization's cybersecurity on an ongoing basis. This activity may include collecting threat intelligence feeds, providing information on potential cyber threats and risks, performing vulnerability scans, performing penetration tests, sponsoring red-team and blue-team exercises, and hunting for known threats or attack patterns within the organization. This team may work with system owners to mitigate identified vulnerabilities through patching, re-engineering, or compensating controls.

Outreach and Training

This team is responsible for conducting outreach with the rest of the organization to promote cybersecurity awareness and education. It keeps track of cybersecurity standards and requirements that apply to employees, partners, and service providers. It prepares documentation and training materials to support this outreach and maintains the materials on an ongoing basis. This team coordinates with the rest of the organization to understand major cybersecurity challenges and tradeoffs. Through effective outreach, this team can help the organization find creative solutions to tough cyber challenges.

Choosing Sub-Function Reporting Structures

These teams do not have to all be under the CISO. They can also be in separate departments, like IT, compliance, or product development. However, they should always have some type of dotted line relationships back to the CISO. Frequently, larger and more complex organizations will have complex cybersecurity reporting structures as well, with cyber sub-functions located in different departments, or perhaps duplicated within different business units or suborganizations. All of these organization approaches can be successful, provided that the lines of authority and responsibility are clearly delineated, and cybersecurity policies are defined, deployed, and enforced.

Balancing Cybersecurity Protection with Other Business Priorities

Once the cybersecurity department is in place, the organization needs to consider the balance between cybersecurity protection and the rest of its business. A lot of this balancing has to do with the consequences of a cybersecurity breach, failure, or compromise. *Would a cyber incident be a devastating existential threat to the organization, or would it simply be an inconvenience or nuisance?* Generally, not all possible cyber incidents are equal – for example, malware on a single employee's computer, versus ransomware holding the entire organization hostage.

The fact is, no matter how big or sophisticated the organization, resources are limited and money spent on cybersecurity must be taken away from money to spend on other areas of the business such as growth, customer acquisition, or investment in new capabilities or infrastructures. These business decisions are never taken lightly, and cybersecurity costs must be contained and controlled.

It is up to organizational leadership to set the right level of funding, and then to deliver the best possible protection within that funding. Some factors to consider when balancing these tradeoffs and finding the right levels of funding for cybersecurity are described below.

Compliance versus Noncompliance

Compliance is a relatively easy business justification, as it is seldom optional for the organization. However, there can be room for interpretation regarding the level of "compliance" to achieve.

- *Barely pass an audit, or pass with flying colors?*
- *Exceed the standard, or hunt for an auditor who will pass you when others might not?*

Leadership should evaluate the security controls required for compliance, the level of controls desired, and the costs required to implement those controls. This cost/benefit analysis can help to define specific cyber projects and the organization's resulting cyber culture.

Calculating the Cost of Cyber Risks

Compliance aside, it may be helpful to consider the business risks associated with cybersecurity.

- *What would the business impact and cost be if confidential information were to be released, or a breach were to occur with regulatory impact?*
- *How much might the resulting fines or the lawsuits cost? What would be the cost to rebuild the IT environment in the case of a ransomware attack or a devastating cyberattack intent on destroying the organization's computers?*
- *What would it cost per hour or per day if organization plants were to go down, or offices were to go dark, computer-wise?*

Understanding these costs can be helpful when considering how much money should be set aside to mitigate cyber risks.

Measuring Risks, Likelihoods, and Impacts

Once the costs of cyber risks are understood, an organization can also use risk management methodology[4] to calculate the value of mitigating those risks. Just as risk management calculates *risk severity* in terms of *risk likelihood* and *risk impact*; risk management can also be used to calculate the business value of *risk mitigation* in terms of the probability the risk will occur and the cost of remediating should the risk occur. Consider the following example calculations:

- A risk with a 10% chance of occurring and a $1 million impact might be expressed as being worth 10% of $1 million, or $100,000 dollars.
- A risk mitigation that reduces the chance of the risk occurring by 50% might be expressed as being worth 50% of the risk's value of $100,000, or $50,000 dollars.

This approach is just one way of calculating values for risks and risk mitigations.[5] These types of simple calculations can be very effective in determining which cyber investments may be worthwhile, while also helping the organization to focus its attention on the cyber investments that can deliver the greatest potential business value, savings, and reduction in measured risk.

Cybersecurity as an Investment

Another way of considering a cybersecurity business case is to look at cybersecurity as an investment in the security of the organization. This viewpoint can be particularly useful for organizations that hold sensitive customer or partner data, where breaches of that data would be extremely detrimental to the organization's reputation. This investment delivers value when the cybersecurity story is told to customers and partners, and can be used as part of the organization's marketing and business development strategy. In this way, the business case for cybersecurity investment might be expressed in terms of potential organization growth, based on a cybersecurity program that improves the organization's position compared to its competitors.

---

4 See Chapter 3, "Cyber Risk Management," for a detailed explanation.

5 Quantitative risk management is an entire field of practice, with entire books written on ways to estimate and combine risk estimates into scientifically valid costs and business values. A thorough treatment of the subject is beyond the scope of this book – for most business needs, the simple calculations we have presented here are sufficient to support smart decision-making.

Budgeting for Protection

Applying the above approaches, the organization can calculate a dollar amount for how much it is willing to spend on its cybersecurity protections, and the value of the risks it is mitigating. These protections and their associated costs must be balanced with other protections (cyber and non-cyber) needed by the organization. These other forms of protection may include physical security, employee and contractor safety, insurance, standards collaboration, regulatory outreach, and political lobbying. Unfortunately, there is no limit to how much money can be spent on these protections – the trick is finding a level of funding that delivers good value within all of the other applicable constraints.

Managing Cybersecurity Costs

An organization could theoretically spend an infinite amount of money on cybersecurity. *So, how does an organization control cybersecurity cost?* By prioritizing expenditures, of course!

In most enterprises, not all IT systems need the same levels of protection, and certainly some users, customers, databases, and backups are more important than others. Cybersecurity does not have to take a "one-size-fits-all" cybersecurity approach, especially when clear lines of delineation can be drawn around the most important, most sensitive, or most vulnerable information systems. To control cyberdefense costs, the chief information security officer (CISO) can use the following cost-reduction *techniques* to reduce the number of systems requiring protection, and the amount of protection required for those systems.

- Tying protection to assets
- Establishing scopes for protection
- Balancing the mix of prevention controls with detection and response controls
- Integrating cyberdefenses and detective control monitoring
- Using open source tools
- Measuring cyberdefense performance

Additional details about these cost-reduction techniques are as follows.

Tying Protection to Assets

By tying protection to assets, an organization can consider the cost of the protection versus the value of the asset being protected. More valuable assets can

justify more expensive protection, while less valuable assets may not. One approach is to budget protection costs as part of the operating costs of the asset involved. For example, allocating manufacturing cybersecurity costs to the manufacturing operations budget, rather than considering such costs as a separate overhead expense. While this approach may in some cases place additional cost pressures on cybersecurity, in other cases, this approach can justify placing additional protections around the most valuable information system assets.

Establishing Scopes for Protection

When there are multiple assets to protect, those assets and their associated information systems may be combined into a "scope" with security protections applied on and around the scope. For example, systems that are subject to the Payment Card Industry Data Security Standard (PCI DSS) or the Health Insurance Portability and Accountability Act (HIPAA) regulation may be isolated from the rest of the organization's IT, and given additional protections appropriate to protecting credit card or medical information. These protections may also include employees and user accounts with access to that data, and not include the rest of the employees in the organization. In this way, cyber controls can be applied to just the limited scope, its systems, and its users, reducing the overall cost and complexity.

Balancing the Mix of Prevention Controls with Detection and Response Controls

Cyber protection needs to consist of more than just trying to block every possible malicious behavior with preventive controls. In fact, trying to block every possible avenue of attack at the network, account, operating system, application, and data levels can rapidly become prohibitively expensive to install and maintain. Robust detection controls and rapid response controls may be cheaper, more effective, and less disruptive to normal IT operations. This balancing approach is especially effective if cyberdefenses can detect and contain attacks after they start, but before they can be completed.

Integrating Cyberdefenses and Detective Control Monitoring

While cybersecurity companies are innovating on a constant basis, more expensive technology does not necessarily translate to correspondingly better protection. Despite decades of people wishing for "silver bullets," no one security technology has shown itself to be 100% successful at blocking all possible cyberattacks, all the time. Frequently, integration of cyberdefenses and monitoring of detective controls is more important to the success of the organization's cyberdefenses, than one or more technologies being "best-in-class" market leaders. By focusing on a well-integrated, multi-layered defense, an organization may be able to achieve protection that is just as good as the "best-in-class" or niche security products, while using cheaper, less-sophisticated components.

Using Open Source Tools

Open source tools are free, and the source code can be modified to suit specific organization needs. *What's the catch?* Open source tools are unsupported, and there may be situations where organization engineers have to go through the source code themselves to understand product behaviors or chase down bugs. Open source tools are a far cry from supported technologies with teams of salespeople, sales engineers, and professional service engineers available to help. But mainstream technologies like the Linux operating system, Elasticsearch analytics, and Nessus vulnerability scanners are widely used and are frequently as mature as commercial products. Some of them are even available as commercial products with full packaging and 24x7 product support. Using technologies like these can save organizations thousands or even millions of dollars per year, without necessarily compromising security.

Measuring Cyberdefense Performance

Another way to control cybersecurity costs is to measure the performance of organization cyberdefenses to see which preventive, detective, response, and recovery security controls are actually being triggered and used. While preventive controls are certainly convenient with respect to blocking cyberattacks, the cost to implement them can be high. To save costs, unused or ineffective controls and the technologies that enable them may be reduced or discarded. Frequently, the biggest hurdle to implementing this cost-saving approach is regulatory requirements and the audits supporting them. However, there is always room to negotiate with

auditors. Organizations can analyze system event logs to show that the unwanted behavior in question is not happening, and that a control to restrict it is not necessary. Auditors may find it acceptable if an organization can demonstrate that it has logs showing that the behavior of concern is not actually occurring, and that if it does occur, the organization will find it quickly enough. By maintaining metrics on how and when security technologies are performing, organizations can understand which technologies are providing critical protection, and which may be redundant or unnecessary.

Effective Cost Management

Using these cost-reduction techniques, an organization may be able to reduce its cybersecurity spending while maintaining acceptable cybersecurity protection, or may be able to increase its cyber protection within a fixed cyber budget. If the business grows and expands, it may become possible to increase cybersecurity spending, particularly if there are increases in cyber assets, threats, vulnerabilities, or risks accompanying the growth. On the other hand, if the business contracts, it may become necessary to reduce cybersecurity spending, even if the risks remain the same. Cyber leadership should remain cognizant of these factors, and be prepared to reduce or increase the organization's cyber spending, as the situation requires.

Cybersecurity spending must be in balance with the rest of the organization's business.

Establishing Cyber Policy Elements

An organization's cyber policy[6] defines what cyber controls are required, and it establishes the foundation for the organization's cyber protections. The policy should be the starting point for all cybersecurity controls, technologies, and processes within the organization. The cybersecurity policy should document what IT assets are to be protected and how well they are to be protected. It should also document what behaviors are and are not acceptable among the people using the organization's IT systems. The policy can set measurable and verifiable standards for the performance of cybersecurity preventive, detective, response,

6 See Appendix C, "Example Cyber Policy" for a detailed example of a policy description.

and recovery controls. These standards may include whether controls are to be performed automatically through technology, or manually through procedures.

An organization's cybersecurity environment can be documented and delivered via cybersecurity policies, standards, procedures, and guidelines, as follows:

- *Policy* documents define what the organization does and does not want to occur, in general terms and without regard to implementation.
- *Standard* documents define thresholds for the delivery and performance of cybersecurity policies, in terms of test criteria that can be passed or failed.
- *Procedure* documents specify approaches and steps for performance that are designed to meet the applicable policies and standards.
- *Guideline* documents provide optional guidance for performance when the publishing organization does not actually have policy enforcement.

Comprehensive cybersecurity policies generally contain combinations of one or more of these types of documentation, and may be published in one combined document or in multiple separate documents. Some additional details about cybersecurity policies, standards, procedures, and guidelines are described here.

Policies

Policies provide the highest level of cybersecurity guidance, and should be written to specify what behaviors are desired or unacceptable. The policy statement does not have to specify how compliance is to be achieved, what level of compliance is desired, or the threshold for determining compliance versus non-compliance. For example, a policy might state that "web browsing will be monitored to detect or block access to inappropriate web sites," or "users of information systems containing sensitive data will be individually identified." The focus of policy statements is to clearly state what behavior is acceptable and unacceptable, and whether that behavior pertains to employees, contractors, partners, guests, or computer information systems.

Standards

Standards supplement policies by providing specific guidance on thresholds for acceptable or unacceptable behavior. A well-written standard is a testable statement where an organization can clearly evaluate if behavior complies or does not comply with the standard. For example, if the standard states that "100% of web browsing will be monitored," then the test fails if a single instance of unmonitored

web browsing can be identified (100% may not be a realistic standard). The standard does not need to specify exactly how compliance is to be achieved – rather, it focuses on how compliance is to be measured. Implementors can then decide on specific technical solutions to achieve compliance. In cases where external regulations or obligations apply, the internal standard should be written to ensure compliance with those external requirements as well.

Procedures

Procedures supplement standards by providing a specific method for compliance with the applicable standards and policies. Procedures will generally apply to the steps people follow, along with the specific technologies or tools they will use, to achieve compliance. While procedures generally outline the steps that people should follow, they may also include engineering documentation describing how IT systems or IT security systems will be configured to comply with the applicable policies and standards. The procedures specify the "how" for compliance by clearly outlining the steps that are to be followed and the sequencing of the steps so the standards are met and the policies enforced. In other words: "If you follow this procedure, you will comply with the policy and meet its standards for performance."

Guidelines

Guidelines provide direction for good practices when there is not a strict policy or standard, or when the organization issuing the guidance does not have authority over the organization receiving the guidance. For example, a multinational organization may have separate, independent corporations in each country, each with its own president or chief executive officer (CEO). In that situation, the central headquarters may provide *guidelines* for the separate corporations, which they can then tailor to be appropriate to their local regulations and requirements. In other cases, specific policies or standards may not apply, but organizations want to provide guidance for good practices to encourage people to be safe or secure. In these cases, such guidance may be written as guidelines. Another example is an organization wanting to provide guidance for "safe and secure use of home computers." While home computers are outside of the organization's authority, secure home computing is most likely in the interest of the organization as well as its employees. In this type of situation publishing guidelines may be both reasonable and appropriate.

Managing Cyber Policy Elements

Although organizations may distinguish policies, standards, procedures, and guidelines as different types of guidance, they do not necessarily have to be contained within separate documents. Frequently, policies and standards can be combined into single documents so that what is desired and the thresholds for success are clear. In addition, different cybersecurity departments may maintain their own policy documentation, resulting in separate cybersecurity policies covering different sub-topics of cybersecurity. In other cases, cybersecurity policies may be incorporated into larger organizational policies, such as for personnel or IT. There is no single "best" approach – what is important is that the appropriate documentation is generated, maintained, followed, and enforced.

Conducting Outreach and Training

Once an organization's cyber policy has been established, standards have been identified, and procedures for compliance have been defined, the next challenge is disseminating the message. *How will people know about the organization's cyber policy if it does not tell them about it?* Through comprehensive outreach and training, employees, partners, contractors, and possibly even customers will know what the cybersecurity policy is, what cybersecurity standards are established, what procedures need to be followed, and what guidelines should be applied so the organization can achieve its cybersecurity goals.

An outreach and training program is seldom a single set of communications – it will likely require multiple sets of communications covering different topics, and targeted to different communities. Communications should reference the applicable regulatory obligations, as well as management's commitments to meeting those obligations. Messages should be posted on internal websites for viewing by employees and partners, and also to public websites where appropriate. Messaging may consist of pamphlets, flyers, banners, and online messaging on computers and connected devices. Messaging should be incorporated into periodic and targeted training for employees, partners, and contractors. The performance of the program should be tracked using metrics and testing to provide management feedback on its breadth and effectiveness. A comprehensive outreach and training program may include some or all of the following components.

Regulatory References

Aspects of a cybersecurity policy that are driven by regulatory requirements should be clearly identified, and those regulatory connections should be reinforced by policy as much as possible. Everyone should understand where noncompliance with the organization's policies can have regulatory impacts that may include fines, penalties, or even criminal prosecution. These connections between the organization's program and its regulatory obligations, as well as the possible consequences for the organization or its employees, should be communicated through the outreach and training program.

Management Communications

Policies come from the top, and cybersecurity policies are no exception. Cybersecurity should be considered alongside other management concerns like personnel safety, protection of equipment and facilities, and delivery of service to customers. Management communications should show that line management is clearly behind cybersecurity efforts and supports the execution of its policies, even when those policies get in the way of convenience, speed, or customer delivery. Management communications should include guidance on "hotlines" for employees to voice concerns or raise alarms. These hotlines may handle cybersecurity concerns alongside of safety, fraud, criminal acts, and other important whistleblower issues.

Internal and External Website Messaging

Once management support is in place, the next place for message dissemination is the web. Internal intranet sites can host copies of policy and procedure documents, provide links to training, and publish statistics on cybersecurity for the organization, its employees, and trusted partners or providers. External, public-facing websites can publish information for the general public, investors, regulators, partners, customers, and contractors. Externally published information may include regulatory references, certificates of compliance, and other materials that would be of interest to external parties concerned about cybersecurity. Organizations want to make sure these materials are all carefully reviewed, free of typos, and consistent with each other. Such materials should also be periodically updated as regulatory requirements evolve, and as policies, standards, and procedures are revised to meet those requirements.

Pamphlets, Flyers, Banners, and Messages

Alongside materials posted to central repositories like internal and external websites, additional supporting materials can be generated to help emphasize the most important points, key messages, and sound bites to remember. Formats for these reinforcement messages can include pamphlets, flyers, banners, and periodic messaging, such as a "security message of the day" or "security tips to remember." Take advantage of login screens, warning screens, and website headers or footers to reinforce security messages. Also important is the review of messages associated with spam warnings, anti-virus alerts, and other tools so they are consistent with other organization messaging. Ensure that messages include appropriate security points of contact and guidance on when and how to call for help.

Training Materials

An excellent opportunity for reinforcing messaging is training materials, whether training is for general employees, specific employee groups like customer service staff, or third parties like partners or suppliers. Make sure these materials are consistent with the rest of organization's security messaging, especially when policies change. While slick multimedia training packages are great, make sure they are easily customizable or changeable in response to new policies, changed situations, or other updates. Otherwise, an organization could find itself in an awkward position where training materials are out-of-date and not in sync with the rest of the cyber outreach and training program.

Metrics and Testing

To help tell the story of outreach, training, and publication efforts, it is helpful to keep track of key metrics so that results can be measured quantitatively. Know what messaging is published where, and how many "page views" or other impressions are occurring. As part of testing, have pop-up quizzes and perhaps even formal tests to capture metrics on training comprehension and attention. Know how many people attend training, how long it takes them to complete the training, and how they do on the test. Know how many people see security banners on the intranet site, how many people see pop-up banners when they logon to their computers or applications, and how many people receive e-mail warning messages. Know how many copies were distributed of flyers, cards, and other handouts, and watch out for stacks of unused materials hiding in office closets.

For every piece of messaging, there should be metrics to help the organization understand how that messaging is being distributed, if the message is being received, and how well it is understood.

Managing Outreach and Testing

With all of this messaging, it is important to keep track of what the messaging is, how it was produced, who the points of contact are to change it, and which aspects of the security policy are reinforced by the messaging. Organizations need to keep track of which messages are easy to change, and which are hard to change. Where automation like content management systems are in use, make sure the outreach and training team has permissions to manage its own content, where practical, rather than being dependent on other teams. Over time, it will become increasingly difficult to keep all of the organization's outreach materials synchronized, or to respond to changes in security policies. Manage this complexity, and stay as agile as possible. In some cases, organizations may find that it is easier to simply delete older messaging that no one reads anymore, rather than trying to keep it up-to-date and synchronized with the messages that are newer and of greater immediate concern.

Reporting Cybersecurity Program Status and Performance

An organization needs to measure its outreach and training program to help ensure that it is accomplishing its goals. While cybersecurity anecdotes are useful – like the story of when the organization's anti-virus stopped the CEO from getting ransomware – security metrics will make or break the business case for the program. An organization needs a combination of stories that describe what security is protecting, along with metrics to show how that protection is progressing over time.

Ideally, there should be metrics for every IT asset to be protected, every cybersecurity control providing that protection, and every user community affected by cybersecurity protections. These metrics should then be collected, compiled, and reported so the organization can holistically visualize the cybersecurity program, its protections, and its performance over time. Be careful of just collecting metrics and then trying to figure out what to do with them – metrics should have a purpose.

Measurement for measurement's sake is a waste of time and money.[7]

There are several steps involved in setting up cybersecurity performance measurement, as follows:

- The first step is *identifying performance indicators* that reflect the organization's threat situation, IT assets, cybersecurity controls, and user communities.
- The second step is *collecting performance indicators* in a manner that is repeatable and not overly onerous, on an ongoing basis.
- The third step is *analyzing performance indicators* to obtain big picture "forest for the trees" visualizations, along with trending over time.
- The fourth step is *reporting cyber program performance* using the performance indicator metrics on a regular basis to employees, management, executives, and other stakeholders so they can act on the information.
- The fifth step is *auditing cybersecurity controls* to collect evidence that the controls are in place and operating as expected.

With these performance measurement steps in place, they can help support audits, assessments, and management of the cybersecurity program. These steps help to enable the organization maintain its program's quality and ensure its compliance with appropriate regulatory and external requirements. Some additional details about these measurement and audit steps are described as follows.

Identifying Performance Indicators

When organizations identify performance indicators for their cybersecurity program, they are looking for metrics that help to reflect their IT environment's assets, threats, vulnerabilities, risks, and mitigations. These metrics can include numbers around an organization's user community, IT environment, major information systems, cloud IT, third parties, and cyber controls. Some of the metrics should be tied to organizational security policies to determine which policies are succeeding and which are challenge areas needing improvement. While the metrics selected are certainly going to evolve, organizations also want to track them over time so they can see trends and answer questions such as:

- *Are cybersecurity challenges getting better or worse?*
- *Are mitigations succeeding or failing?*

7 Donaldson, S.E., and S.G. Siegel. *Successful Software Development*. 2nd Edition. Upper Middle River, NJ: Prentice Hall PTR, 2001.

- *Which trends indicate good news? Which trends indicate concerns?*
- *What actions can be taken to reverse the concerning trends?*

Answers to such questions can help shape the organization's cybersecurity program over time and remain responsive to the evolving cyber landscape.

Collecting Performance Indicators

Once performance indicators are identified, they must be collected. Ideally, most of the metrics should be automatically collected, or collected using highly repeatable and easy-to-perform manual procedures. Inevitably, some organizational metrics are going to be challenging to collect, or to collect reliably. These types of metrics may be good candidates for less-frequent collection, rather than trying to track them regularly. Organizations will have to find an acceptable balance of workload versus value to collect the information needed. The indicator collection tempo should be tuned to sync with reporting schedules, as well as management decision cycles. In practice, weekly, monthly, quarterly, and annual collection rates tend to work well. A good rule of thumb for metrics is as follows:

- *Weekly metrics* should reflect ongoing security operations.
- *Monthly and quarterly metrics* should support operational trending, resource management, and strategic planning.
- *Annual metrics* should support strategic and financial decision-making.

Analyzing Performance Indicators

Once performance indicators are collected consistently, organizations will want to analyze them. Analysis should seek to draw from the numbers answers to questions like the following:

- *Is our security working or not?*
- *What do the performance indicators mean?*
- *Are there performance indicator trends?*
- *Does the organization need to take some action? What action? When?*
- *What could go wrong? Will we know when things go wrong?*

The analytical challenge is to turn the numerical *data* into *actionable intelligence* that can be used to make *informed decisions* and take *meaningful actions* to manage resources and improve security. Give particular attention to analysis that helps to show trends in the threat situation, risk posture, and overall

cyberdefense performance. Frequently, these trends will be obtained by fusing together multiple other metrics to try to understand the "big picture."

Reporting Cyber Program Performance

When metrics have been collected and analyzed to tell the cybersecurity story, the next step is to get the message out. Performance metrics and analysis should be incorporated into regular weekly, monthly, quarterly, and annual reports to reflect the cybersecurity stories the organization needs to know. Such stories should also be incorporated into other reporting channels, like intranet websites, organization public websites, internal messaging, and training materials, as appropriate. There is nothing wrong with having the organization's e-mail gateway report that "spam is up 20% this year" while warning users of potentially malicious e-mail messages, or having the organization's web gateway warn users that "over 300 people went to malicious websites last month" while blocking a web link. These metrics help non-cyber people to visualize the significance of the cybersecurity threats and the magnitude of the cyber risks faced by the organization.

Auditing Cybersecurity Controls

Once cybersecurity performance metrics are in place, the next component of a performance management program is an audit of organization security controls. An audit is a process to collect evidence indicating that controls are in place and are operating as expected. The audit process may be a spot check of a report, or it may be an automated search for control violations or operational variances. Organizations can audit preventive, detective, response, and recovery controls. Frequently, control performance metrics are integral parts of the audit process. The results of the audit may then be fed into compliance attestations to satisfy regulatory or contractual requirements. By performing control audits regularly, organizations should have a comprehensive understanding of how well their cyberdefenses are working, where the deficiencies lie, and how things could be improved.

Managing Cyber Program Status and Performance

When combined with performance indicator metrics and cybersecurity incidents, audit results should provide the organization with a thorough picture of its entire cybersecurity program's status and operation. By tracing these results

back to cybersecurity business drivers – including regulatory, compliance, and contractual obligations – the organization can tell the story of why it is doing cybersecurity, and how well the organization is doing in satisfying its cybersecurity obligations. By telling the story in this manner, an organization should be able to make a compelling business case for where cybersecurity is needed, to what degree it is needed, and what operational tradeoffs are acceptable in pursuing cybersecurity objectives.

Chapter 7
Cybersecurity Capabilities

Earlier chapters describe cyber topics including threats, daily challenges, risk management, program management, cybersecurity security controls, and various protection concepts. This chapter builds upon these cyber concepts and describes how they, along with others, can be used to define an organization cybersecurity program. Figure 7.1 depicts the major topics of this chapter.

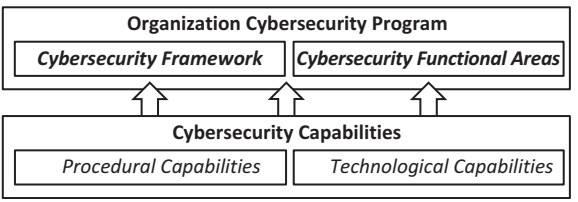


Figure 7.1: An organization's cybersecurity capabilities, both procedural and technological, form the foundation for its cybersecurity program.

This chapter introduces the concept of *cybersecurity capabilities* and defines them in terms of their procedural and technological components. The chapter then introduces an *organization cybersecurity framework* concept by describing example cybersecurity frameworks. The chapter details the framework concept in terms of its major components – architecture, policy, programmatics, IT life cycle, and assessments. The chapter then provides a detailed description of the *cybersecurity framework architecture* in terms of *cybersecurity functional areas*, which group together related cybersecurity capabilities to lay the foundation of an organization's cybersecurity program. Finally, the chapter provides a detailed description of the cybersecurity functional areas in terms of their key features, goals, overall objectives, likely threat vectors they defend against, and corresponding *representative* cybersecurity capabilities.

Cybersecurity Capabilities

NIST Special Publication (SP) 800–53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, describes the idea of security capability as an abstraction as follows.

https://doi.org/10.1515/9781501506529-007

> . . . security capabilities can address a variety of areas that can include, for example, technical means, physical means, procedures means, or any combination thereof . . . it is important for organizations to have the ability to describe **key security capabilities** [emphasis added] needed to protect core organizational missions/business functions . . . security capability provides a shorthand method of grouping security controls that are employed for a common purpose or to achieve a common objective. This [functional grouping] becomes an important consideration, for example, when assessing security controls for effectiveness.

In this book, a *cybersecurity capability* is defined as a process or technology that enables the organization to perform a specific control. Cybersecurity capabilities can be either procedural or technological, as described here:

- *Procedural capabilities* are delivered by having a person follow an approved procedure on a set schedule or in response to an action. Even though procedural capabilities are powerful, they do not scale like a piece of technology. However, procedural capabilities are most likely an organization's most powerful ones. An organization's actual security against a professional attacker is almost entirely dependent on its people, not its technology.
- *Technological capabilities* are provided by technologies installed into the organization's infrastructure. A single technology may provide multiple capabilities. For example, a single technology can block an attack and raise an alert that an attack occurred. Technologies may also provide cybersecurity capabilities across multiple functional areas. Technology capabilities are powerful because once they are deployed, they tend to "just work" – at least until they break and stop working. However, technology needs to be carefully engineered, deployed, managed, and monitored if it is really going to live up to its potential.

Organization Cybersecurity Frameworks

There are a number of excellent cybersecurity frameworks that have been developed over the past two decades. A few examples of such frameworks are briefly described as follows.

International Organization for Standardization (ISO) 27001/27002 Version 2013

The ISO created the ISO 2700 series of standards to address the topic of organizational information security.[1] ISO 27001 is the specification for an organization information security management system (ISMS), and ISO 27002 is the code of

1 https://www.iso.org/isoiec-27001-information-security.html

practice for information security controls. Organizations can be accredited for ISO 27001 by following a formal audit process that includes independent certification by an outside auditor.

Australian Defense Signals Directorate (DSD) Strategies to Mitigate Targeted Cyberintrusions

The DSD publishes a list of 37 strategies to mitigate targeted cyberintrusions.[2] This framework emphasizes the "Top 4" mitigation strategies believed to thwart more than 85% of cyberintrusions. These strategies are: application whitelisting, patching applications, patching operating system vulnerabilities, and restricting administrative privileges.

Payment Card Industry Digital Security Standard (PCI DSS) Version 4.0

The PCI DSS version 4.0 is a set of requirements for protecting cardholder data for organizations handling credit card data on their IT systems.[3] PCI DSS includes a set of mandatory security controls that must be employed by all certified entities processing credit card transactions or data.

Cybersecurity Maturity Model for Certification (CMMC)

The U.S. Department of Defense (DoD), Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD A&S) developed the CMMC framework "in concert with DoD stakeholders, University Affiliated Research Centers (UARCs), Federally Funded Research and Development Centers (FFRDCs), and the DIB [Defense Industrial Base] sector."[4] This framework provides a standardized format for measuring and reporting cybersecurity maturity across organizations.

Health Insurance Portability and Accountability Act (HIPAA) of 1996

HIPAA established national standards for the use and protection of electronic protected health information (EPHI). The HIPAA security rule specifies requirements for protecting the confidentiality, integrity, and availability (CIA) of EPHI at healthcare providers, clearinghouses, insurance plans, and drug dispensers. NIST published "An Introduction Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule" (SP 800–66 Revision 1), October 2008 to help organizations understand and comply with these requirements.

2 https://www.emtdist.com/solutions/australian-signals-directorate-top-4-mitigations/
3 https://www.pcisecuritystandards.org/
4 https://www.acq.osd.mil/cmmc/docs/CMMC_Model_Appendices_20200203.pdf

(ISC)^2 Common Body of Knowledge (CBK)

The International Information Systems Security Certification Consortium, Inc. (ISC)^2 created the CBK as a core knowledge base for training Certified Information Systems Security Professionals (CISSP).[5] CISSP is one of the most widely used cybersecurity certification programs. While not a security framework per se, the CISSP training curriculum provides a comprehensive, organized framework for discussing and teaching cybersecurity topics.

Organization Cybersecurity Framework Components

These frameworks, along with many others, can provide organizations with potential components for inclusion into their cybersecurity programs. To be successful, these many components should be organized into an overall framework, should be coordinated with each other, and should work well with minimal redundancy, overlap, or complexity. Figure 7.2 introduces an *organization cybersecurity framework* to help organizations integrate such cybersecurity components.[6]

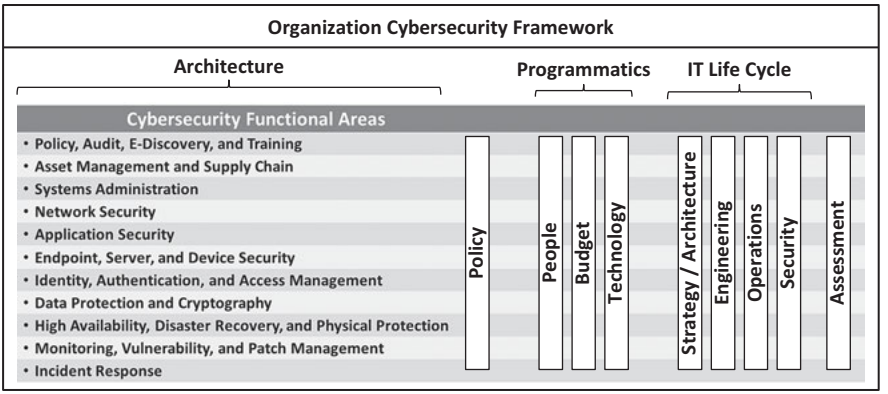


Figure 7.2: A comprehensive cybersecurity architecture provides a foundation for integrating organization policy, programmatics, IT life cycle, and assessments.

This framework consists of the following components.

---

5 https://www.isc2.org/Certifications/CBK

6 Figure 7.2, Figure 7.3, and associated text are adapted from Donaldson, Siegel, Williams, and Aslam. *Enterprise Cybersecurity Study Guide*, Apress, 2018. This organizational cybersecurity framework has been "field-tested" and "field-proven" for managing cyberdefenses against the most dangerous nation-state attackers.

Architecture

The architecture component consists of cybersecurity functional areas that are used to organize and manage organization cybersecurity. Each functional area is comprised of cybersecurity capabilities. As new capabilities emerge and become important, they can be added to the appropriate functional area. Obsolete or ineffective cybersecurity capabilities can be removed. Functional areas help track, manage, and delegate cybersecurity capabilities throughout an organization.

Policy

The policy component directs what is to be protected and to what degree, as well as the consequences are for policy violations. Staffing, budget, technology, and operations should trace to written policy. Linking these policy factors together provides a foundation for the entire cybersecurity program. These policy factors can be detailed through organization standards, guidelines, processes, and procedures.

Programmatics

The programmatic component consists of the following elements:

- *People* responsible for cybersecurity who are organized by different IT departments such as operations, cybersecurity, compliance, or internal audit. People must be carefully organized so that their authority, responsibility, and expertise are in harmony with each other. Organizational lines of authority must be carefully considered, along with organizational interfaces where departments must collaborate.
- *Budget* is the allocation of resources to pay for deploying, operating, and maintaining the cybersecurity technologies and operational processes making up a well-thought-out cybersecurity program. The amount of money allocated to each cybersecurity element must be adequate so that the element can be effective.
- *Technology* protects the organization by providing prevention, detection, logging, response, and audit capabilities. The reality is that the size, complexity, and speed of modern IT dictate that most cybersecurity cannot be accomplished manually. The right technologies, well-deployed and properly maintained, are essential for successful cyberdefenses.

IT Life Cycle

The IT life cycle component consists of the following elements:

- *Strategy/Architecture* helps ensure the technologies are well-coordinated so they work together as integrated systems. Cybersecurity technologies need to be well-coordinated with the rest of IT and the organizational elements

the technologies support. Strategic and architectural disconnects can render technologies ineffective, impair organizational productivity, or dramatically increase operational costs.

- *Engineering* helps ensure technologies are properly selected to meet organizational requirements, are configured and deployed correctly, and are supported so the technologies continue to meet initial and new requirements throughout their life cycles. Engineering also helps ensure deployed systems are "fit for purpose" and "fit for use" for as long as they are needed and used.
- *Operations* help ensure IT infrastructure technologies are efficiently and cost-effectively operated according to formal service level agreements (SLAs). Security technologies must be regularly updated to stay effective, and other security operational processes (such as policy exception management) must also be performed. If cybersecurity is not maintained on an ongoing basis, it will quickly become obsolete.
- *Security* helps ensure that cyberdefenses (e.g., preventive, detective, response, and recovery controls) are properly implemented, monitored, and maintained, as well as cybersecurity operational processes and technologies. Security also supports cyber control audits and assessments to understand how controls function and whether they are effective. Security responsibilities span the entire IT life cycle to help ensure that cyber protections are considered, refined, tested, and implemented as needed.

Assessment

The assessment component evaluates the effectiveness of the organization's risk mitigations, cybersecurity capabilities, and operational processes. Assessment includes reporting against legal, regulatory, and compliance requirements. It ensures that organizational cybersecurity measures up to the expectations of the organization's applicable external obligations.

Cybersecurity Framework Architecture

Effective cybersecurity is not just about buying the latest technology and implementing it, nor is it just about people, defenses, or a series of checklists. Effective cybersecurity balances and integrates technology, processes, people, organization, budgets, and compliance requirements in a cost-effective manner. The architecture provides the "foundation" upon which the other major framework components are "connected." As shown in Figure 7.3, this architecture consists of functional areas containing cybersecurity capabilities.

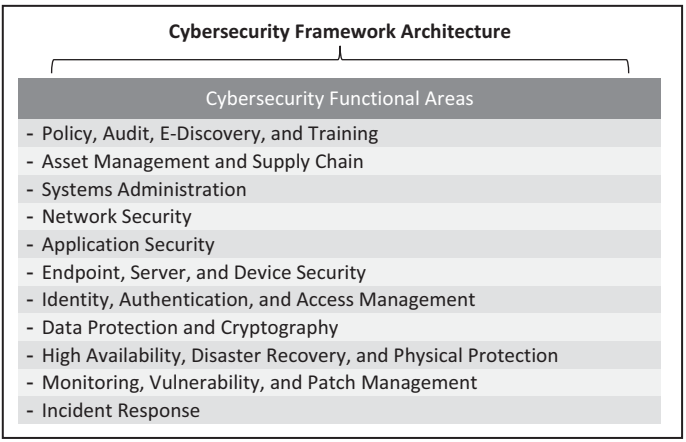


Figure 7.3: Cybersecurity functional areas are used to organize cybersecurity capabilities together into a comprehensive cyber architecture.

The remainder of this chapter briefly describes the architecture functional areas shown in Figure 7.3. Each functional area is described in terms of a short definition, goal, objective, threat vectors, and some representative cybersecurity capabilities.

Policy, Audit, E-Discovery, and Training

This functional area deals with the governance of cybersecurity policy, audit, e-discovery, and training. The functional area groups together various security oversight functions – including mapping security controls to meet compliance requirements – along with some secondary functions regarding personnel security and privacy concerns. Key functional area features include the following:

- Policy sets the organizational strategy for all the other functional areas, while the audit function periodically reviews the other functional areas to ensure compliance with policy and effectiveness of preventive and detective controls.
- The chief information security officer (CISO) office oversees the audit program, which periodically reviews preventive, detective, and monitoring controls to verify their operation and effectiveness. The CISO office also oversees external e-discovery reporting requirements and organization cybersecurity training.

- The CISO office interfaces with the legal department to support e-discovery measures as required by regulation, legislation, or litigation.
- This functional area oversees training for employees, IT, and security personnel to help ensure that they are properly informed of their responsibilities and are prepared to perform them on an ongoing basis.

This functional area is the home of the CISO executive, who would have authority and responsibility for the overall organizational cybersecurity program. Generally, it makes sense for a single department to perform these functions, rather than having the functions spread across different departments.

Goal

The goal of this functional area is to address the people, policy, regulatory, and compliance aspects of cybersecurity.

Objective

The overall objective of this functional area is two-fold: (1) control of organizational processes and capabilities, and (2) management of programmatic and personnel issues associated with process and capability deployment.

Threat Vectors

Threat vectors include the following:

- Security management gaps that result in processes or capabilities being neglected, causing security risks.
- Compliance management or reporting gaps resulting in external audit findings.
- Personnel security gaps resulting in untrustworthy personnel in positions of organizational trust, also known as insider threats.
- Training and accountability gaps resulting in the organization's staff knowingly or unknowingly performing risky cybersecurity behaviors on a regular basis.

Representative Cybersecurity Capabilities

The capabilities in Figure 7.4 provide oversight of controls and audit of their effectiveness, support for legal e-discovery activities, and training of staff in proper security policies and practices. The capabilities account for compliance requirement and mapping security controls to meet those requirements. In addition, the capabilities involve the security control audit program that periodically reviews preventive, detective, and monitoring controls to verify their operation and effectiveness.

Figure 7.4: Representative cybersecurity capabilities for the *Policy, Audit, E-Discovery, and Training* functional area.

These capabilities include the following:

1. *Governance, Risk, and Compliance (GRC), with Reporting* involves managing the overall cybersecurity program, risk management process, and reporting against external requirements. This capability enables the cybersecurity program to fit in with the rest of the organization's business risk management efforts.
2. *Compliance and Control Frameworks (SOX, PCI, Others)* involve identifying the organization's compliance obligations, the controls required for that compliance, and the frameworks for organizing those controls and their outputs. This capability enables the organization to cross-map and translate from its operating cyber controls to its compliance reporting.
3. *Audit Frameworks* involve establishing a structure for conducting internal and external audits of cyber controls and their performance, for the satisfaction of the organization's compliance requirements. This capability enables the organization to have a single audit team or external auditor perform audits that satisfy multiple compliance requirements, as well as to track audit deficiencies from their identification through to their eventual remediation.
4. *Customer Certification and Accreditation (C&A)* involves performing formal processes to satisfy customer requirements; they may be characterized as C&A or other types of contractual obligations. This capability may be required to satisfy customer or partner requirements for deploying new IT systems, for reviewing already-deployed IT systems, or to perform formal contract acceptance for delivery (and payment).
5. *Policy and Policy Exception Management* involves managing the organization's cyber policies, as well as having a process for granting and tracking exceptions to policies. This capability helps to ensure policies are drafted, disseminated, and maintained. This capability also tracks exceptions to policies so they can be risk-managed and reviewed periodically.

6. *Risk and Threat Management* involves performing formal tracking of the organization's risks and cyber threats, ideally using methodology that integrates with the organization's other business risk management efforts. This capability enables the organization to establish structure around its cyber risk management efforts, and to consider cyber threats and risks alongside of its other business concerns.
7. *Privacy Compliance* involves managing the organization's compliance requirements related to protecting the privacy of its employees, partners, customers, and other interested parties. This capability has become more important with the passage of privacy regulations like General Data Protection Regulation (GDPR) in Europe and California Consumer Privacy Act (CCPA) in California.
8. *E-Discovery Tools* involve having the technical ability to conduct legal e-discovery investigations, when directed by legal counsel. This capability may be almost non-existent at smaller organizations not involved in legal proceedings, while for larger organizations it may be the full-time job of an entire department.
9. *Personnel Security and Background Checks* involves looking into the security of the organization's personnel, particularly trusted IT and cybersecurity personnel. This capability may involve coordination with recruiters, human resource (HR) staff, industrial security personnel, or the office of the chief security officer (CSO).
10. *Security Awareness and Training* involves building and disseminating materials for training the organization's personnel on cybersecurity, security awareness, regulatory obligations, and other concerns. This capability enables the security organization to leverage the larger organization community as a "force multiplier" for successful cyberdefense.

Asset Management and Supply Chain

This functional area provides for the tracking of organizational assets, procurement information associated with them, their life cycles, changes, and ensuring orderly and secure disposal without compromising the organization's data or security.

Goal

The goal of this functional area is two-fold: (1) ensure the organization knows what IT assets it has, and (2) manage supply chain risks from acquisition through operation to disposal.

Objective

The overall objective of this functional area is to ensure that operational staff follow proper procedures that are supported by various technical capabilities.

Threat Vectors

This functional area is about managing unknown threats to organization assets, what happens to those assets while they are in the organization, where those assets came from, and where they are going to when they leave the organization. This functional area protects against numerous unknown threats, some obvious and some not so obvious. Threat vectors include the following:

- The ability of an attacker to place components in the organization without those components being noticed. This threat can be physical devices connected to the network, or it can be software installed on organizational computers or network-connected devices.
- Unauthorized changes or reconfigurations of systems are dangerous threats. Asset management needs capabilities to be able to detect such threats. Some of these capabilities may overlap with other functional areas, but it is often logical to have the overall supervision of change management centralized with the asset management functional area or team.
- Attackers compromising products through suppliers and then getting those compromised products into the organization. Such products may simply be of lower quality than expected, or they may be fully weaponized to attack the organization from within.
- Attackers leveraging the supplier ecosystem to attack the organization. Frequently, suppliers are trusted with access to organizational resources, but oftentimes, supplier security to protect those organizational resources is not as diligent as the organization protecting its own resources.
- Insecure disposal resulting in the leakage of sensitive organization data. Just as "dumpster diving" can be used to obtain significant information about an organization, so can obtaining disposed electronics that have not been properly sanitized.

Representative Cybersecurity Capabilities

The capabilities in Figure 7.5 ensure that organizational assets are accounted for over their life cycle, are made compliant with organization policies, and are properly disposed of at end of life. These capabilities also help ensure assets are obtained from trustworthy suppliers.

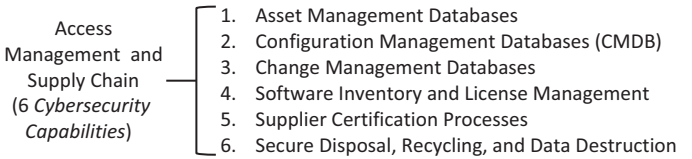


Figure 7.5: Representative cybersecurity capabilities for the *Asset Management and Supply Chain* functional area.

These capabilities include the following:

1. *Asset Management Databases* involve tracking the organization's IT physical, logical, and network-connected assets, so they can be accounted for and protected. This capability is important if protections are to be comprehensively deployed, and information assets are to be protected from their deployment until their retirement.
2. *Configuration Management Databases (CMDB)* involve tracking the configuration, relationships, and sub-components of IT assets, and linking IT systems with the organizational structure of the people maintaining them. This capability enables the organization to rapidly navigate IT systems and identify the human points of contact to be involved in cyber activities.
3. *Change Management Databases* involve tracking changes to IT systems within the organization, along with their lifecycle, approval, and completion. This capability may be delivered by a single system that includes CMDB functions as well – it can help the organization identify changes that may be of cybersecurity concern, along with changes associated with malicious or negligent activity.
4. *Software Inventory and License Management* involves tracking software and licenses used by the organization. This capability is important for the organization to satisfy its software compliance obligations, but can also be leveraged to identify unauthorized and malicious software installed on organization systems.
5. *Supplier Certification Processes* involve tracking the organization's suppliers and performing due diligence to make sure they are able to comply with the organization's security and compliance requirements. This capability also includes keeping track of third-party suppliers, so their personnel can be tracked, provisioned, and de-provisioned within organization IT systems as appropriate.
6. *Secure Disposal, Recycling, and Data Destruction* involve performing secure disposal of organization IT systems at the end of their lifecycle. These topics are of particular concern for systems like personal computers, servers, copiers,

and IoT devices that may contain sensitive or proprietary data. This capability involves arranging for the deletion or destruction of sensitive data, along with safe disposal of equipment in an environmentally friendly manner.

Systems Administration

This functional area provides for secure administration of organization infrastructure and security systems, and protects systems administration channels from compromise. Systems administration gets its own functional area because if it is compromised or fails, an attacker can easily disable and bypass the rest of the organization's security.

Goal

The goal of this functional area is to protect the organization's administrative channels from being used by an adversary.

Objective

The overall objective of this functional area includes the following complementary objectives:

- *Preventive* objective makes it harder for attackers to get systems administration control, slows attackers down so they are easier to catch, and makes it easier to catch the attacks when they happen.
- *Detective* objective focuses on detecting attacks on systems administration channels and malicious systems administration activity when it occurs. Detective controls need to be configured to alert on patterns associated with malicious systems administration activity and attacks on privileged administrator accounts. It may also involve the manual review of certain systems administration activities to ensure they are legitimate and appropriate.
- *Forensic* objective focuses on creating detailed audit logs of all privileged systems administration activities. These logs can then be used to generate detective control alerts, facilitate regularly scheduled audits, and support investigations of incidents.
- *Audit* objective focuses on generating artifacts and evidence that systems administration is not malicious in the organization. Audits can be regularly scheduled, but unscheduled reviews of systems administration activities can also help ensure such activities are legitimate. Audits do not have to be elaborate. An audit as simple as checking which accounts logged onto what hosts at what time can be very effective at catching malicious activity in a timely fashion.

Threat Vectors

This functional area involves keeping attackers (including insiders) from conducting malicious systems administration activities in the organization. Threat vectors include the following:

- Systems administrator credentials that attackers can use from compromised machines inside the network.
- Systems administrator computers that attackers can use to impersonate legitimate privileged users.
- Systems administration infrastructure such as computer management, patch management, network management, or other administrative channels that attackers can use to take control of the organization.
- Computing infrastructure such as virtualization, storage, or keyboard-video-mouse (KVM) consoles that attackers can use to take control of systems.
- Monitoring systems with administrative access to the organization that attackers can use to take control of systems.
- Local computer administrative accounts that attackers can use to move from one personal computer to another with administrative rights.

Representative Cybersecurity Capabilities

The capabilities in Figure 7.6 make it harder for attackers to get administrative access, make attackers easier to detect and stop if they get control, isolate command and control networks and protocols, provide cryptographic protection for systems administrators, and allow for systems administration activities to detect attacks.

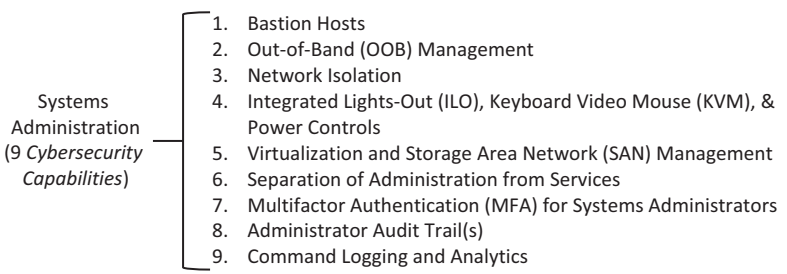


Figure 7.6: Representative cybersecurity capabilities for the *Systems Administration* functional area.

These capabilities include the following:

1. *Bastion Hosts* involve using isolated, hardened computer systems for privileged systems administration, especially management of sensitive security

systems and their protections. This capability protects against many types of attacks against organizations' infrastructure and can be particularly effective when used within a network segmentation strategy.

2. *Out-of-Band (OOB) Management* involves performing systems administration over separates or isolated management connections. This capability may be implemented through physical isolation, logical isolation, or protocol-level separation.
3. *Network Isolation* involves using a separate "telemetry" network for performing sensitive systems administration. This approach is particularly important for telecommunications providers where the operations network is an integral part of the service they deliver to their customers. This capability uses networking technologies and protocols to isolate systems administration functions from operations, customer, and other delivery network traffic.
4. *Integrated Lights-out (ILO), Keyboard Video Mouse (KVM), & Power Controls* involve using remote, possibly network-based technologies to deliver key datacenter management functions. This capability enables administrators to remotely power up, power down, and connect to datacenter infrastructure possibly located hundreds or thousands of miles away.
5. *Virtualization and Storage Area Network (SAN) Management* involves management functions for the organization's computing and storage infrastructure. This infrastructure may be used to bypass network and operating system protections and possibly access sensitive data without authentication or detection. This capability should lock down such access to only highly trusted personnel and systems, so that software and application security controls are enforced to the maximum extent possible.
6. *Separation of Administration from Services* involves designing IT systems so that systems administration functions cannot be performed using the same connections as the delivery of services. This capability provides additional layers of protection around administration functions, above and beyond user permissions or user account authentication.
7. *Multifactor Authentication (MFA) for Systems Administrators* involves enforcing MFA for system administrators, so that privileged account abuse requires more than just compromising a username and a password. This capability can be very powerful when MFA for systems administrators is enforced along with changing administrator passwords after every time they are used. Privileged Account Management (PAM) technologies are one way of delivering these capabilities in an easy-to-use and intuitive fashion.
8. *Administrator Audit Trail(s)* involve tracking privileged administrator accounts, their logons, and their activity when they are used. It should be performed in conjunction with periodic audits of administrator accounts to

detect inappropriate activity or possible administrator account compromise. This capability relies on having comprehensive logs of administrator logons and systems administration activities.

9. *Command Logging and Analytics* involves logging the commands of systems administrators and performing analytics on those commands to detect signs of administrator account compromise or abuse. This capability may be delivered through manual logs, manual review procedures, or through PAM technologies, if they are deployed.

Network Security

This functional area provides for the security of an organization's networks, their services, and access to these networks from the internet or internally connected devices. Network security examines data traversing the network to detect intrusions against the network and connected computers, using preventive, detective, and monitoring controls to defend the network. Network security can include segmenting the network to contain attacks and provide defenders with opportunities to stop attacks before they proceed too far. Network security can also involve filtering and monitoring the organization's network traffic to block malicious traffic and detect attacker communications.

Goal

The goal of this functional area is to protect the organization's network from use or attack by an adversary.

Objective

The overall objective of this functional area includes the following complementary objectives:

- *Preventive* objective is to block malicious traffic from passing from one part of the network to another, or channeling that traffic so it can be detected through other means.
- *Detective* objective is to monitor and analyze network traffic to identify malicious traffic while it is in transit.
- *Forensic* objective is to log information about network traffic, or possibly all of the network traffic itself, so that it can be analyzed by detective controls to support investigations and audits.
- *Audit* objective analyzes network traffic to identify malicious activity or generate artifacts indicating the lack of malicious activity.

Threat Vectors

This functional area involves attackers using the network in some way and relying on the network to perpetuate their attack while it is in-progress. Threat vectors include the following:

- Outbound network connections from servers or clients on the internal network to remote attacker-controlled systems.
- Network connections of internet-facing servers, which can be used to establish command-and-control channels into the organization.
- Internal networks that attackers can use to move laterally among computers inside the organization.
- External network connections that can be used to extract and remove data from the organization.
- Network infrastructure components that can be used to gain entry to the organization or to bypass other security measures.

Representative Cybersecurity Capabilities

The capabilities in Figure 7.7 are not "silver bullets" that satisfy all cybersecurity requirements. Experience of the past decade has shown that network security alone is not enough to thoroughly protect an organization. However, network security continues to be an important functional area that can block, detect, and intercept many potential attacks.

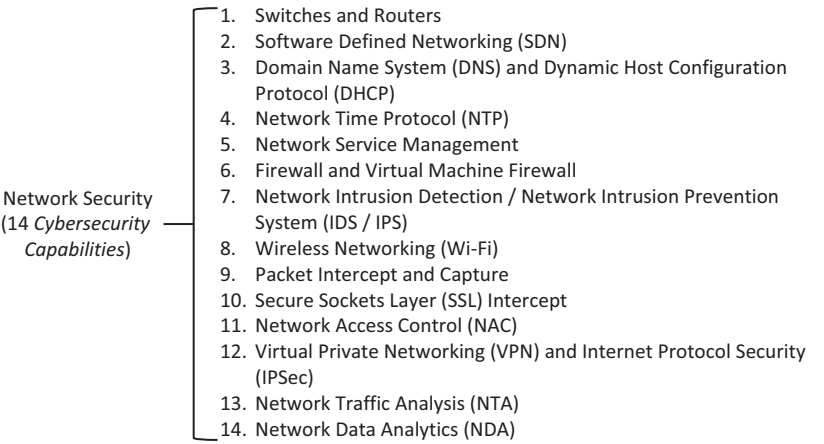


Figure 7.7: Representative cybersecurity capabilities for the *Network Security* functional area.

These capabilities include the following:

1. *Switches and Routers* involve managing the network infrastructure supporting the organization's IT infrastructure. This capability ensures that network

traffic is properly routed through cybersecurity functions like firewalls and intrusion detection devices, to provide critical network defenses.

2. *Software Defined Networking (SDN)* involves using software to define network architectures, connections, and capabilities, particularly within cloud environments. This capability enables the entire network to be specified "as code" and rapidly configured or re-configured to satisfy operational and cybersecurity requirements.
3. *Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP)* involve delivering naming and host configuration services to the network. These capabilities are of particular cybersecurity concern, because they are foundational to the network and can be easily manipulated to bypass or subvert other network security measures.
4. *Network Time Protocol (NTP)* involves having a single "source of truth" for the organization's IT systems clocks and timing. This capability is essential for proper timestamping of security logs and is also needed for certain security protocols like Kerberos authentication.
5. *Network Service Management* involves establishing secure channels for managing the organization's network and network infrastructure. This capability may be implemented using vendor management tools, through secure systems administration channels, or through cloud service providers.
6. *Firewall and Virtual Machine Firewall* involve establishing security enforcement points around key organization network boundaries, as well as around virtual machines within virtualized and cloud infrastructures. This capability is a fundamental network security function, and works closely with security strategies like network segmentation.
7. *Network Intrusion Detection/Network Intrusion Prevention System (IDS/IPS)* involves filtering to detect (IDS) and block (IPS) known malicious network traffic patterns. This capability may be able to detect signs of attacker penetration, command-and-control, lateral movement, or data exfiltration across the organization's networks.
8. *Wireless Networking (Wi-Fi)* involves securing wireless networks so they are authenticated, access-controlled, and protected from potential abuse. This capability is important because wireless networks may permit attackers to target and attempt connections to organization networks from outside the organization's facilities and physical protection boundaries.
9. *Packet Intercept and Capture* involves being able to record large volumes of network traffic across key network boundaries, such as internet-bound traffic or traffic between applications and databases. This capability permits reconstruction of network exchanges that can be very helpful to investigating known or suspected cyber incidents.

10. *Secure Sockets Layer (SSL) intercept* involves being able to intercept encrypted SSL and transport layer security (TLS) connections to be able to read the plaintext network traffic contained within. This capability is essential against modern attack techniques that encrypt their communications across the internet and organizational network boundaries.
11. *Network Access Control (NAC)* involves identifying, profiling, and authenticating network-connected devices before they are permitted access to the organization's network, even when "plugged in" within the organization's own facilities. This capability can work with perimeter network defenses to provide comprehensive protection against rogue and unauthorized network-protected devices.
12. *Virtual Private Networking (VPN) and Internet Protocol Security (IPSec)* involve providing secure channels for external connection to the organization's network for the purposes of remote access, data interchange, partnership, and collaboration. This capability should be protected using strong, multifactor authentication, and may be deployed in conjunction with network access control and other forms of policy enforcement.
13. *Network Traffic Analysis (NTA)* involves analyzing network traffic patterns to identify malicious connections, suspicious data flows, and attempts at bulk data exfiltration. This capability establishes baselines of "normal" traffic patterns and can be very effective at flagging network behaviors outside the baseline for follow-up investigation.
14. *Network Data Analytics (NDA)* involves performing advanced analytics against network metadata, traffic flows, encryption certificates, and other parameters, to identify network behavior that may be of concern. This capability takes network traffic analysis (NTA) further by performing analysis against additional parameters above and beyond just network traffic patterns and data flows.

Application Security

This functional area provides for the security of organizational applications using security technologies that are specific to the particular application technologies and their communication protocols. The applications most needing additional security are the ones that communicate over the network and are accessible from the internet. By this simple definition, application security technologies and capabilities include e-mail security, application-aware firewall features, database gateways, and application-specific web proxies.

Goal

The goal of this functional area is to protect the organization's applications from use or attack by an adversary.

Objective

The overall objective of this functional area includes the following complementary objectives:

- *Preventive* objective is to block exploitation of applications and application communications protocols from malicious use.
- *Detective* objective is to detect compromises of applications and attempts to exploit them for malicious purposes.
- *Forensic* objective is to log data about application activity that can be used for audits and investigations of incidents.
- *Audit* objective is to collect evidence and artifacts that suggest applications are safe and are not being used or manipulated by attackers.

Threat Vectors

Targeted and general threats seek to exploit the organization's applications in some way, particularly the internet-connected applications such as e-mail and web browsing. Some organization applications may be custom-built, and securing those applications can be particularly challenging. Application security threat vectors include the following:

- E-mail messages may contain attachments or links that use vulnerabilities in other applications, such as picture viewers or document viewers, to gain control of endpoint computing devices such as personal computers or mobile devices.
- Web browsers and web plug-ins may contain vulnerabilities that are exploited to gain control of users who go to malicious websites. Attackers can compromise a legitimate website and use it to serve up malware to unsuspecting visitors.
- Organization server applications, such as web application servers, can be exploited to take control of those servers and get inside the organization's IT infrastructure.
- Flaws within in-house organization application software (such as web, mobile, or desktop applications) can be used to gain entry into the organization, compromise data stored within the applications, or target the organization's employees or customers.

Representative Cybersecurity Capabilities

The capabilities in Figure 7.8 provide protections that are tailored to specific applications and include e-mail filtering, web proxies, web application firewalls, and database firewalls. An organization's application developers need to use proven

methodologies to ensure that custom applications are not vulnerable to attack practices such as SQL injection or cross-site scripting.

Figure 7.8: Representative cybersecurity capabilities for the *Application Security* functional area.

These capabilities include the following:

1. *E-mail Security* involves applying protections to e-mail coming into and going out of the organization's e-mail infrastructure. This protection can include spam filtering, anti-virus scans, attachment filtering, and hyperlink checking. This capability is vitally important as e-mail has become a major source of malware and malicious attacks against organization personnel.
2. *Webshell Detection* involves being able to detect attacker remote access tools installed onto internet-facing web servers. A webshell allows an attacker to run arbitrary commands on a server using a single webpage, hidden among the organization's website. This capability is important to protect against hidden command-and-control connections that can be used for remote control or data exfiltration.
3. *Application Firewalls* involve network-based firewalls that are aware of the specific application, and able to filter on application data above and beyond just network parameters. This capability enables the organization to perform application-specific filtering and protect against malicious or accidental application misbehavior.
4. *Database Firewalls* involve network-based firewalls that specifically process database connection and administration traffic. They are often deployed between application servers in the demilitarized zone (DMZ) and back-end database servers that might be on the internal network. This capability can protect against attempts to target the database servers, bypass data encryption protections, or exfiltrate database records.
5. *Forward Proxy and Web Filters* involve filtering web requests originating from organization computers and requesting web pages from the rest of the internet. This capability can analyze such traffic for specific patterns including malicious websites, malvertising, and web-based command-and-control connections.

6. *Reverse Proxy* involves filtering web requests originating from the internet destined for web and application servers on the organization network (usually in the DMZ). This capability protects internal web servers from direct internet connections and can block many types of attacks attempting to exploit vulnerabilities in their web pages, applications, or software.
7. *Data Leakage Protection (DLP)* involves monitoring network traffic for patterns matching specific types of data that may be of concern, like customer names, account numbers, or social security numbers. This capability, while it may generate large numbers of false positives, can detect employees accidentally (or deliberately) mishandling sensitive data, as well as attackers attempting to perform mass data exfiltration.
8. *Secure Application and Database Software Development* involves putting in place rigorous methodology for developing secure software throughout the organization's software development life cycle (SDLC). This capability may be enforced by development tools, configuration controls, or the organization's own software path to production.
9. *Software Code Vulnerability Analysis* involves performing static and dynamic analysis of software code to detect bugs, vulnerabilities, and areas of concerning software behavior. This capability can then be leveraged to drive subsequent vulnerability scans, follow-up security checks, and line-by-line code reviews to protect against security errors in deployed code.

Endpoint, Server, and Device Security

This functional area provides for the protection of endpoint computing devices – such as personal computers, servers, and mobile devices – that access organizational data. This functional area also involves detecting when endpoint defenses are breached.

Endpoint, server, and device security can **never** be assumed to be 100% effective, as administrators will make mistakes, viruses will proliferate, and zero-day vulnerabilities will always be obtainable by well-resourced attackers.

Goal

The goal of this functional area is threefold: (1) prevent attackers from taking administrative control of computing devices, (2) detect attempts to maliciously use computing devices, and (3) facilitate the investigation of incidents when compromises are suspected.

Objective

The overall objective of this functional area includes the following complementary objectives:

- *Preventive* objective is to make endpoints, servers, and devices harder to compromise in the first place. Endpoint security "hardens" system operating systems and software so they are difficult to breach and exploit.
- *Detective* objective is to alert the organization about malicious software and attempts to exploit the operating system, so defenders can identify systems that are either compromised or under attack.
- *Forensic* objective is to log device activities securely so there is an audit trail for investigations. Activity logs can include system configurations, administrator commands, and changes to operating system security features. Forensics may also include the complete imaging of systems for detailed forensic analysis.
- *Audit* objective includes analyzing logs to identify malicious activity or to create artifacts indicating the absence of malicious activity on audited systems. Security audits may include analyzing systems to gain confidence that they are operating properly and are free of malicious software.

Threat Vectors

Attacks focus on taking control of endpoints within the organization. There are countless ways to take control, and creative attackers are constantly creating new attacks methods and attack vectors. Threat vectors include the following:

- Malware that proliferates across the internet, exploiting operating system vulnerabilities to pass from machine to machine. This prevalent problem is mostly due to unpatched vulnerabilities (i.e., not keeping up-to-date with the latest security patches), particularly in application software that may not be centrally managed.
- Deliberate attackers that exploit vulnerabilities in an organization's software products or operating systems to conduct targeted attacks against specific organizations to compromise their computers or devices. Such attackers may also leverage obscure, recent, or zero-day exploits to take control of targeted computers or devices.

Representative Cybersecurity Capabilities

The capabilities in Figure 7.9 provide protection for endpoints, servers, and other devices. In practice, these capabilities may be delivered through different technologies, depending on the type of endpoint device to be considered. Endpoint security needs are slightly different, depending on whether the endpoint is a personal computer, server computer, virtual machine, mobile phone, tablet, or smart network-connected device.

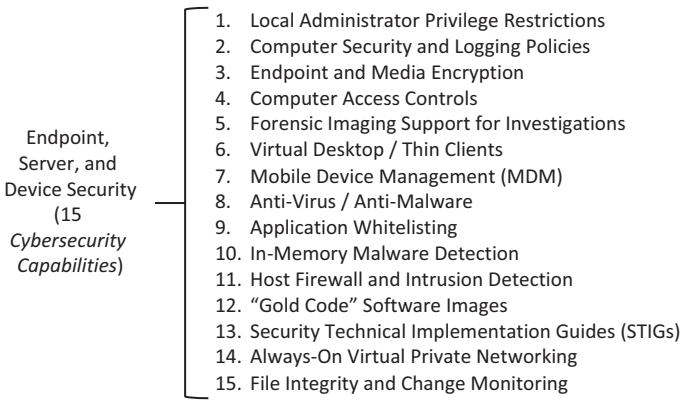


Figure 7.9: Representative cybersecurity capabilities for the *Endpoint, Server, and Device Security* functional area.

These capabilities include the following:

1. *Local Administrator Privilege Restrictions* involve restricting the ability of regular computer users to use "administrator" privileges to install unauthorized software, disable security protections, or otherwise re-configure organization endpoint computers. This capability can block cyberattacks that rely upon attempting to trick users into installing the attackers' tools or backdoor software.
2. *Computer Security and Logging Policies* involve configuring endpoint and server computers to log security-related data, and usually to then send that data in to central log-collection infrastructures. These logs can then be used by security investigators to identify attacker footholds, attempts at lateral movement, or other malicious behavior.
3. *Endpoint and Media Encryption* involves encrypting hard drives, fixed storage, and removable media that may contain organization proprietary data. This capability is very useful for laptops, mobile devices, and portable storage like "thumb drives," since encrypted data is unreadable on lost or stolen devices.
4. *Computer Access Controls* involve placing access restrictions on computers, servers, and mobile devices so only identified and authorized users may login to them. This capability is commonly implemented using usernames and passwords tied to enterprise directories, but may also be enforced using multifactor authentication like tokens or smart cards.
5. *Forensic Imaging Support for Investigations* involves installing tools on organization devices that can capture "forensic" images of running programs, system memory, and fixed storage like hard drives. This capability enables investigators to take snapshots of the full configurations of possibly

compromised systems, and then analyze those images for signs of compromise or malicious behavior.

6. *Virtual Desktop/Thin Clients* involve placing organization applications and data inside of a virtualized client interface or a "dumb" thin client terminal. This approach allows the organization to avoid actually letting users store sensitive data on their laptop computers or personal devices, since the data stays within the organization-controlled system and is only displayed on the users' personal device screen. This capability is very effective at protecting against data leakage from users attempting to store personal copies of sensitive data, database downloads, or other proprietary organizational data.
7. *Mobile Device Management (MDM)* involves placing software on mobile devices that access or store organizational data like e-mail, calendar, or shared files. The MDM software then establishes secure connections to organizational IT systems and encrypts local copies of organizational data. This capability ensures that proprietary data is protected on the mobile device, and can even remotely wipe the device if necessary.
8. *Anti-Virus/Anti-Malware* involve scanning the storage (hard drives or solid state) of computers or servers, looking for patterns corresponding to known malicious software. These tools may also monitor the programs that are run from the storage for potentially malicious behavior or malicious code. This capability is very effective at catching known malicious software, as well as "commodity threats" traversing the internet.
9. *Application Whitelisting* involves monitoring the software programs running on computers or servers, and only permitting explicitly authorized programs to run. Authorized programs may be identified using digital signatures, hash codes, or other patterns that are explicitly identified by policy (the "whitelist"). This capability is very effective at locking down systems for maximum security, although it requires that whitelists be constantly updated to contain the latest versions of the authorized software. As a consequence, it tends to be better suited for servers that don't change often, than for personal computers or mobile devices that are being constantly updated.
10. *In-Memory Malware Detection* involves scanning the memory of computers, servers, and devices to detect in-memory malware. This type of malware is injected directly into the computer's running memory and does not reside on the hard drive or fixed storage. This capability can detect and block advanced attacks that may not be caught by traditional anti-virus, anti-malware, or application whitelisting capabilities.
11. *Host Firewall and Intrusion Detection* involves placing hardware and intrusion detection capabilities directly onto individual host computers or servers. This capability allows the organization to enforce its network security

policies on systems that are outside of the network perimeter and directly connected to the internet, such as from home networks, partner connections, or cloud computing.

12. *"Gold Code" Software Images* involve maintaining strict configuration control of software intended to be installed on organization servers, computers, and mobile devices. This capability protects these software images from attack or compromise, and makes sure that changes to the software are properly tested and approved.
13. *Security Technical Implementation Guides (STIGs)* establish formal procedures for configuring security policies on endpoint and server computers. These configurations may involve disabling unused services, removing unnecessary software, and loading settings to "harden" running programs against potential compromise. This capability should be used to configure organization endpoints and servers in a consistent and secure fashion, before they can be used in production.
14. *Always-On Virtual Private Networking* involves configuring mobile computers – particularly laptops that may be taken outside of the building – to always send their network traffic through the organization's secure network perimeter. This capability permits the organization's network security controls to monitor all traffic in and out of these devices, and to enforce network security protections (like firewalls, reverse proxies, and IDS/IPS) at all times and for all organization computing devices.
15. *File Integrity and Change Monitoring* involves monitoring computer or server file systems to detect unauthorized changes to files, configuration settings, or other parameters. This capability can be very effective at catching changes outside of approved change control processes, as well as attackers installing malware or disabling security protections on compromised computers or servers.

Identity, Authentication, and Access Management

This functional area provides support to the organization's cyberdefenses by providing answers to the following questions:

- *Who is accessing the organization's IT systems?*
- *How does the organization identify people accessing its IT systems?*
- *What IT systems can people access once they are authenticated?*

When systems are isolated on organization networks, the answers to these questions are often a matter of who has physical access to the organization's facilities.

With physical isolation, it is expected that those who have access to the facilities and networks will be cleared and authorized in some way. However, once systems are connected to the internet, this connection becomes a tremendous problem, as billions of people are potentially just a click and a password away from accessing organization systems. The problem becomes even more acute when data and IT services are installed "in the cloud" at facilities completely outside of the organization's control. This reality is where identity management and solid authentication mechanisms become critical to successful cyberdefense.

Identity management helps ensure that accounts and accesses are provisioned, de-provisioned, and periodically re-certified according to organizational policies. Authentication helps ensure that appropriate technologies are used to positively identify users who are accessing organizational systems, so there is a high level of confidence that the users are who they say they are. Access management helps to ensure that privileges on organizational systems are provisioned and de-provisioned according to "least privilege" mythologies, and users do not receive privileges that exceed their roles in the organization.

Goal

The goal of this functional area is to ensure that only authorized people can access organizational resources. Complicating this goal is the fact that people, resources, and permissions change over time. Large numbers of people and resources – along with huge numbers of potential access permissions, all of which are in constant flux – make this goal extremely challenging to execute.

Objective

The overall objective of this functional area includes the following complementary objectives:

- *Preventive* objective is to make it harder for attackers to gain access to organizational resources by impersonating legitimate users, granting themselves inappropriate permissions, or using accounts that should not have been available to them.
- *Detective* objective is to alert the organization about account, credential, or permission abuse within the organization, and to identify when accounts are being attacked or have been compromised.
- *Forensic* objective is to log account activity, including the full life cycle associated with accounts, permissions, and log-on activities. These logs can then be analyzed and correlated with other logged events to identify attack patterns.
- *Audit* objective involves processing logs to create artifacts and gather evidence that accounts and permissions are not being abused. Achieving this

objective with a reasonable level of confidence requires a thorough audit trail and cross-correlation with information from other sources, such as endpoints and applications.

Threat Vectors

Credential abuse is one of the most common vectors for targeted attackers to gain organizational access and accomplish their goals. It is relatively easy for attackers to get username and password credentials and then use them in an organization, particularly if the organization allows remote access without multifactor authentication. Once attackers start using legitimate credentials, many organization defenses are avoided because those defenses focus on activities other than those of "legitimate" or "authenticated" users. Account and privilege management are extremely difficult to do well, and this area is relatively "soft" for attack – even in the most professional organizations. Threat vectors include the following:

- Accounts that are no longer used or maintained, but have not been actually removed from the organization.
- Legitimate credentials that attackers obtain and then use to gain entry to the organization. Once entry is achieved, attackers escalate their privileges by exploiting vulnerabilities in endpoints, applications, or networks.
- Weak authentication methods or protocols that attackers exploit to impersonate legitimate users.
- Weaknesses in privilege management that attackers us to take regular user accounts and grant those accounts administrative or other super-user privileges within the organization.

Representative Cybersecurity Capabilities

The capabilities in Figure 7.10 center around managing the full identity and access life cycle, and making identities and authentication available to the full range

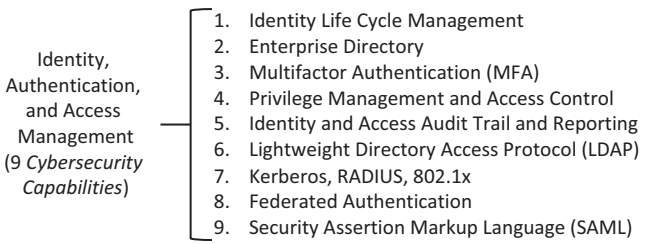


Figure 7.10: Representative cybersecurity capabilities for the *Identity, Authentication, and Access Management* functional area.

of organization systems that support them. Identity and access management technologies and deployments can easily become complex, multi-million-dollar undertakings.

These capabilities include the following:

1. *Identity Life Cycle Management* involves managing the life cycle of organization electronic identities, through creation, modification, and eventual deletion. This applies to employee identities, as well as contractors, partners, customers, privileged systems administration accounts, and system or service accounts used for system-to-system authentication. This capability is sometimes called *identity governance*, and serves as the foundation of the identity and access management program.
2. *Enterprise Directory* involves making the right identities available to the right applications at the right time. This capability may include *meta-directories* that tie together multiple sets of identities and make them available to internal and external applications.
3. *Multifactor Authentication (MFA)* involves protecting the user login process with multiple factors – usually a password or personal identification number (PIN) that the user knows, along with a physical token, smart card, or mobile device that they have. This capability may also include use of biometric features like fingerprints or facial recognition.
4. *Privilege Management and Access Control* involves managing the access and permissions of user accounts and electronic identities against organization IT systems. This capability may include using *role-based access control* (RBAC) or *attribute-based access control* (ABAC) to ensure the right users have access to the right data at the right time.
5. *Identity and Access Audit Trail and Reporting* involve logging and reporting who accesses what within the organization's IT systems, and making those logs available for audit and review. This capability is foundational to most compliance audits and audit reporting.
6. *Lightweight Directory Access Protocol (LDAP)* involves delivering directory functions using the LDAP protocol, which has become a de facto standard across most IT environments. This capability usually serves as the foundation for user authentication to organization computers and applications.
7. *Kerberos, RADIUS, 802.1x* involve delivering authentication functions using these protocols, usually to support secondary functions in the organization's IT environment. Kerberos has become popular in the Microsoft operating system environment, while RADIUS and 802.1x are usually used for authentication to network devices and wireless networks. This capability is usually directly connected to the organization's primary LDAP directories.

8. *Federated Authentication* involves delivering mutual authentication with trusted partners so that organization identities and authentication can be used at partner IT systems. This capability is particularly important for cloud services, where a single cloud provider may support hundreds or thousands of customers, each with their own authentication requirements.
9. *Security Assertion Markup Language (SAML)* involves delivering federated authentication using the SAML protocol, which has become a de facto standard for most cloud-based authentication. This capability is an open standard that is widely available and supported.

Data Protection and Cryptography

This functional area provides for the protection of data stored in the organization and the use of cryptographic technologies to perform that protection. These capabilities can then be used to support other operations such as authentication, nonrepudiation, and data integrity. This functional area is becoming increasingly important, and has evolved from a specialized niche protecting military communications to protecting almost every aspect of modern internet communications, commerce, and transactions. Cryptography is also critical to the success of strong authentication technologies such as digital certificates, smart cards, and one-time password tokens. This functional area must contend with the rapid rate at which cryptographic standards and technologies are evolving. Cryptography that took a thousand years to crack a decade ago may only take weeks or days to crack today. Cryptography presents many unique challenges that require specialized expertise to understand and evaluate effectively.

Goal

The goal of this functional area is to protect the confidentiality and integrity of data using cryptographic techniques and technologies.

Objective

The overall objective of this functional area includes the following complementary objectives:

- *Preventive* objective involves protecting the confidentiality and integrity of organizational data by using cryptographic technologies. The effectiveness of these technologies generally revolves around the algorithms used and the protection the technologies provide for cryptographic keys.

- *Detective* objective involves monitoring organization cryptographic use to detect weak cryptography, compromised keys, or cryptographic breaches when they occur.
- *Forensic* objective involves tracking the cryptography used in the organization and logging what algorithms and keys are used where, to support later investigations.
- *Audit* objective involves collecting information on the cryptography and keys that are used and their strengths. It involves ensuring that they meet the organization's requirements and applicable external standards for strength and protection.

Threat Vectors

It is important for organizations to pay attention to cryptography and either have or externally obtain the expertise to ensure that cryptography is utilized effectively. Threats include the following *attacker actions*:

- Using encrypted web sessions either into or out of an organization to control computers on the inside so those sessions are more difficult to monitor.
- Encrypting organization data and then demanding a ransom be paid to get the keys to decrypt the data.
- Cracking weak cryptography to steal credentials, intercept encrypted sessions, or read encrypted data.
- Using brute force to compromise passwords or data that have been protected using weak cryptography.
- Stealing the keys to strong cryptography if those keys have not been well-protected.
- Using "code signing" certificates to make malware appear to be a legitimate application or device driver.
- Stealing data at rest or in-transit while it is unencrypted, either through the application itself or at other vulnerable points in time.

Representative Cybersecurity Capabilities

The capabilities in Figure 7.11 require three things to be accomplished correctly:

- The application of cryptography must be carefully coordinated with the overall life cycle of the data to be protected.
- Cryptographic algorithms must be chosen that are secure and will stay secure for the life of the protected data.
- Cryptographic keys must be properly generated and then protected from compromise from generation to disposal.

Data needs to be protected, but also available when it needs to be used. When data is decrypted so it can be used, it must be protected by other means.

Figure 7.11: Representative cybersecurity capabilities for the *Data Protection and Cryptography* functional area.

These capabilities include the following:

1. *Secure Sockets Layer (SSL) and Transport Layer Security (TLS)* involve protecting sensitive communications over insecure networks like the internet, usually using digital certificates to verify the identity of one or both ends of the communications. This capability is essential to the security of web-based e-commerce; more recently, user privacy concerns have made its use common on all types of commercial websites.
2. *Digital Certificates (Public Key Infrastructure [PKI])* involve using cryptographic keys to uniquely identify individuals, computers, and websites on the internet. This capability relies upon *key pairs* consisting of private keys and corresponding public keys, that are mathematically related to each other. The *public key* is then placed into a *digital certificate* from a trusted PKI *certificate authority*. Recipients of the certificate can then do cryptographic operations to verify the identity of the individual, computer, or website presenting the certificate, and then use it to authenticate or establish secure communications.
3. *Key Hardware Protection (Smart Cards, Trusted Platform Modules [TPMs], and Hardware Security Modules [HSMs])* involve using highly specialized technology to protect the *private keys* used in PKI, along with other *symmetric keys* used for performing high-speed encryption and decryption of secure data. This capability protects the keys so they cannot be copied or stolen, even if attackers have remote control of the computers involved in the transactions.
4. *One-Time Password (OTP) and Out-of-Band (OOB) Authentication* involve using cryptography to generate secure codes for users to authenticate to

online systems, instead of using static passwords that can be copied and abused. This capability involves either changing the password every time it is used (OTP) or delivering the password separately over a secure channel (OOB). Both of these methods are frequently used for multifactor authentication, along with PKI certificates.

5. *Key Life Cycle Management* involves systematically managing keys, certificates, and other cryptographic materials used in the enterprise, throughout their lifecycle from creation to deletion. This capability is particularly important when keys need to be rotated to protect them from compromise, or cryptographic algorithms need to be updated across the organization's IT environment.
6. *Digital Signatures* involve using cryptographic methods to protect data from unauthorized changes, and to verify the identity of the party presenting the data. This capability may be used to protect logfiles, certificates, online documents, internet e-mails, or digital identities used on the internet. With digital signatures, the recipient can perform cryptographic operations and have a high level of confidence that the data is legitimate and has not been changed since it was originally signed.
7. *Complex Passwords* involve creating user passwords that are difficult to guess, not composed of dictionary words, and resistant to cryptographic attacks. The best complex passwords are completely random, which makes them secure but difficult to memorize. This capability involves using strong, complex passwords where appropriate, and may include *password managers* or *privileged account managers* to manage those passwords and make them easy to use for regular users and systems administrators, alike.
8. *Data Encryption and Tokenization* involves using cryptographic methods to protect secure data when it is transmitted or stored. *Data encryption* involves encoding data using cryptographic algorithms and encryption keys, while *tokenization* involves randomizing data without changing its format.[7] This capability is essential to protecting sensitive or proprietary data, and may be used on backup tapes, hard drives, databases, applications, and communications connections.

---

7 Using tokenization, the phone number 800-555-1212 might be encoded as 903-826-1705. While the format of the digits remains the same, the data values have been encoded. The algorithm can later be reversed to get the original value back. This is a very useful technique with non-production systems where an organization wants to protect production data, but does not want to have to re-engineer software code that assumes particular formats for the data to be processed.

9. *Brute Force Attack Detection* involves being able to detect when attackers are attempting to guess user passwords through *brute force attacks* that try large numbers of password possibilities until they get it right. Attackers may use dozens, hundreds, thousands, or millions of passwords, until they succeed. This capability involves designing internet-facing systems to be able to detect attackers making large numbers of unsuccessful password attempts, and then take action to block the attackers from connecting. Multifactor authentication, because it adds an additional authentication step, can be very helpful here as well.
10. *Digital Rights Management (DRM)* involves using cryptographic tools to protect data going outside of the organization and enforce *digital rights* on those who try to view that data. DRM is tied to the document, and may include e-mail, spreadsheets, presentations, and text file formats. This capability requires those who wish to view the document connect back to the organization and verify their identities. Once the organization confirms that they are authorized to view it, the document is decrypted and made visible.

High Availability, Disaster Recovery, and Physical Protection

This functional area provides for keeping the organization's IT services available for use by its legitimate users. An *availability* cyberattack attempts to deny access to those services, usually through denial of service (DoS) attacks, distributed denial of service (DDoS) attacks, or other attacks on the IT infrastructure. Such attacks may involve disabling IT systems either temporarily or permanently, denying their availability to intended users. This functional area involves making IT systems highly available and easily recoverable should a problem occur. This functional area also provides for physical protection of facilities, people, systems, and data.

Goal

The goal of this functional area is to satisfy organizational requirements for the continuity of operations in the face of adversity, which may range from mild, routine failures of computing devices to severe natural or human-made catastrophes.

Objective

The overall objective of this functional area is to ensure the organization has the ability to respond to a wide range of potential adverse situations. Perhaps most important, an organization needs to consider how these reaction capabilities might serve the organization in the event of a cyberattack, among other potential threat scenarios.

Threat Vectors

Primary threats in this functional area can include availability cyberattacks, regular mechanical wear and tear, natural circumstances that are outside of anyone's control, or human-led activities that are either negligent or malicious. Threat vectors include the following:

- Scheduled maintenance where systems administrators take systems offline for upgrades or patches and potentially disrupt operations.
- Regular wear and tear or hard-to-predict circumstances, resulting in organization IT systems failing unexpectedly.
- As a result of a cyberattack, the integrity of certain IT systems is placed sufficiently into question that restoring or rebuilding the systems from backups is warranted. This may also include resetting their data back to a known-good state with questionable transactions reversed.
- As a result of a cyberattack that is in-progress, it becomes desirable to activate contingency capabilities to provide either additional capacity or to allow for the reconfiguration of primary systems to defend against the attack.
- A natural or human-made disaster results in the loss of a primary data center or other operational systems. As a result, organization services must be failed over (switched over) to a secondary site. This transition to a secondary site is subject to recovery point objectives (RPO) and recovery time objectives (RTO).[8]
- A deliberate attack, such as an act of war or a sophisticated criminal act, results in the physical destruction or impairment of facilities required for operations.

Representative Cybersecurity Capabilities

The capabilities in Figure 7.12 center on making IT systems more robust, replicating the same data to multiple locations, and physically protecting the devices and storage containing organization data and systems. While this functional area primarily deals with availability, it may also consider data confidentiality and integrity as well.

---

8 Recovery point objective (RPO) is the point in time that data is recovered through. For example, if the recovery point is nightly, then a recovery will not include transactions from the following day. Recovery point is about how up-to-date data needs to be. Recovery time objective (RTO) is how long it takes from when the disaster is declared until the system has been recovered and its data and transaction processing capabilities are available again.

Figure 7.12: Representative cybersecurity capabilities for the *High Availability, Disaster Recovery, and Physical Protection* functional area.

These capabilities include the following:

1. *Clustering* involves running applications across two or more computers simultaneously, with the computers staying synchronized so one can take over for the other if a failure occurs. This capability permits one member of the cluster to be taken off-line for maintenance, or due to a failure, while the other continues delivering service. Clustering is essential for high availability services that are expected to be available 100% of the time.
2. *Load Balancing, Global Server Load Balancing (GSLB)* involve distributing computing load across two or more supporting systems, with GSLB permitting those systems to be geographically separated at different locations. This capability helps organizations scale services up to hundreds or thousands of delivering servers, and can also be used in conjunction with clustering to permit maintenance across parts of the environment – one or more systems can be taken offline while the load balancers distribute the workload to the other systems that remain operational.
3. *Network Failover, Subnet Spanning* involve designing datacenter networks so the same network can reside at multiple locations, with data seamlessly transmitted across both locations as if they were co-located. This capability can be used in disaster recovery scenarios to permit seamless failover to backup locations while primary production systems continue to run.
4. *Virtual Machine Snapshots and Cloning* involve being able to backup the configurations of virtual machines – sometimes while they are still running – and transfer those configurations to other locations. This capability can be used to replicate virtual machine functions at alternate locations, and also to "roll back" configurations to previously used settings, in the event of a problem or a failure.
5. *Data Mirroring and Replication* involve making multiple copies of production data or databases (mirroring) and then keeping them synchronized as

transactions or changes occur (replication). This capability can be used to maintain multiple copies of user databases and transactions, to protect against transactions getting "lost" in the event of a failure, and to reduce the time needed to switch over to backup systems in an emergency.

6. *Backups and Backup Management* involve making backups of production data, applications, and system configurations, and then tracking and managing those backups so they can be recovered when needed. This capability is foundational to disaster recovery plans but can also be used for configuration management and other types of contingency planning.
7. *Off-Site Storage* involves storing copies of critical data away from primary production sites, to guard against failures or natural disasters. This capability should be applied not only to production data, but also to software code, system configurations, database schemas, and cryptographic keys.
8. *Facilities Protection* involves placing security preventive and detective controls around organization facilities, datacenters, and other physical locations. Data that is protected online, but stored in insecure facilities, may still be vulnerable to attack, theft, or compromise. This capability should be carefully coordinated among cybersecurity, physical security, organization management, and other interested parties.
9. *Physical Access Controls* involve placing access protections around important facilities and the information assets they contain. Access controls may include badges, gates, doors, and guards for secure locations. This capability involves placing one or more layers of physical protection around the most important people, information systems, and data belonging to the organization.
10. *Physical Security Monitoring* involves emplacing sensors, alarms, cameras, and other monitoring around the most sensitive facilities and physical locations. Critical assets should be protected using *double barrier protection*, where access is protected by two layers of physical access control, with the space in between them monitored for intrusions.

Monitoring, Vulnerability, and Patch Management

This functional area provides for the regular monitoring of security infrastructure, scanning and analysis of vulnerabilities in that infrastructure, and management of patches and workarounds to address those vulnerabilities. By performing these functions, this functional area enables the organization to maintain its cybersecurity posture, and also to detect when that posture has issues that need to be addressed.

Goal

The goal of this functional area is to understand how security changes over time and maintain the organization's security posture on an ongoing basis. Risk must be constantly re-assessed, as vulnerabilities that were not a major concern yesterday may become a critical concern today.

Objective

The overall objective of this functional area includes the following complementary objectives:

- *Preventive* objective is to ensure vulnerabilities are identified, mitigated, and patched before they can be exploited by attackers.
- *Detective* objective involves monitoring the organization's security systems to detect incidents so that they can be promptly investigated and remediated.
- *Forensic* objective involves logging event and incident information to support subsequent analysis and investigation.
- *Audit* objective involves centrally collecting audit trails that can be used to support compliance requirements.

Threat Vectors

This functional area is about operational processes that maintain the organization's cyberdefenses and catch threats before they prove disastrous. Threats include the following *attacker actions*:

- Leveraging attack methods that are not detected or that are detected by unmonitored systems and are invisible to defenders.
- Exploiting vulnerabilities during the time window between when they become known and before they can be patched.
- Targeting security and logging infrastructure to block or delete records of their activities so that those activities become invisible to defenders.
- Taking advantage of an organization's inability to cross-correlate attacker activities that are monitored and logged, resulting in the organization being unable to recognize or respond to the attack.

Representative Cybersecurity Capabilities

The capabilities in Figure 7.13 focus on maintaining the organization's security on an ongoing basis and actively detecting incidents against organization security systems. These capabilities can be summarized as follows:

- *Monitoring capabilities* provide for the collection and analysis of logging data from the infrastructure, then processing that data to identify events of interest. Given events of interest, the organization identifies specific incidents that require investigation and remediation.

- *Vulnerability capabilities* involve scanning organizational infrastructure and computers to identify vulnerabilities in software or configuration so that identified vulnerabilities can be remediated.
- *Patch management capabilities* help ensure the ongoing patching of commercial products so the products can be kept current with the latest security fixes and enhancements.

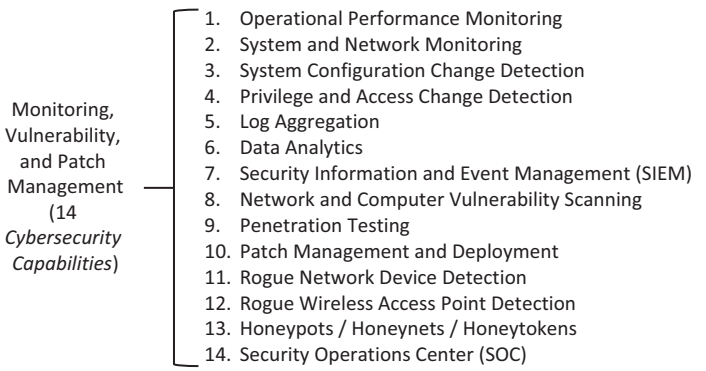


Figure 7.13: Representative cybersecurity capabilities for the *Monitoring, Vulnerability, and Patch Management* functional area.

These capabilities include the following:

1. *Operational Performance Monitoring* involves monitoring the operations of IT systems to detect system outages caused by cyberattacks or performance impacts caused by compromise or system tampering. This capability is useful for detecting many types of malicious behavior, particularly ransomware and cryptomining.
2. *System and Network Monitoring* involves monitoring the availability and capacity of systems and networks making up the operational IT environment. This capability may be able to detect system outages caused by cyberattacks, along with command and control network traffic, lateral movement across network boundaries, and attempts to exfiltrate large amounts of data outside the organization.
3. *System Configuration Change Detection* involves monitoring the configuration files and settings on IT systems to detect unauthorized and possibly malicious system changes. This capability can be delivered as part of the overall IT change management program, and then shared with cybersecurity.
4. *Privilege and Access Change Detection* involves monitoring the privileges and access controls of user accounts, particularly against sensitive infrastructure, cybersecurity, or regulated IT systems. This capability may be able to detect cyberattacks involving creation of rogue accounts or attempting privilege escalation.

5. *Log Aggregation* involves bringing together logs from large numbers of IT and cybersecurity systems into a single chronological log stream that can then be further analyzed. This capability provides the organization with a single view of its activity, enabling the type of global, correlated, visibility needed for investigating advanced cyberattacks.
6. *Data Analytics* involves performing multidimensional analysis of logs and operational data to find patterns indicative of cyberattacks. This capability may be used to detect attacks based on complex multivariable detection factors, or to pursue attacks through advanced analysis of log data.
7. *Security Information and Event Management (SIEM)* involves collecting logs and then performing cross-correlation among the log entries so that timestamps are synchronized and data fields are unified. With correlation, information like network addresses, computer names, and user accounts can be extracted from multiple log sources and linked together into a complete picture This capability makes it easier to track activity across many different types of devices and search for attacker indicators organization wide.
8. *Network and Computer Vulnerability Scanning* involves scanning the organization's services, networks, and computing devices for known vulnerabilities and missing patches. This capability may be performed manually on-demand, or automatically by scripted tools according to a set schedule. Identified vulnerabilities should be tracked, mapped back to system owners, and prioritized for patching or remediation.
9. *Penetration Testing* involves using attacker toolsets and techniques to attempt to penetrate the organization's cyberdefenses, testing out its preventive and detective controls (but hopefully not the recovery controls). This capability should ideally be done by an external third party, according to carefully defined parameters and rules of engagement.
10. *Patch Management and Deployment* involves identifying software patches for organization computers and applications, and deploying those patches regularly to address performance or security issues. This capability goes hand-in-hand with vulnerability scanning and configuration control, as many software vulnerabilities require patches for remediation, and deploying patches into production environments requires careful testing and a methodical path to production.
11. *Rogue Network Device Detection* involves scanning organization networks for rogue devices that may have been installed by an attacker or negligent insider. These might include insecure or personal devices, unauthorized equipment, or inappropriate use of the organization's own computers. This capability makes it possible to detect these devices, trace their location, and empower the right people to investigate them.

12. *Rogue Wireless Access Point Detection* involves being able to detect unauthorized, or rogue wireless networks installed in organization facilities. This capability is important because rogue wireless networks may be insecure, improperly secured, or abused to allow data to escape the organization's facilities and protected network environment.
13. *Honeypots/Honeynets/Honeytokens* involve installing components meant to attract and deceive attackers. Honeypots are servers configured to appear to be attractive legitimate infrastructure, while actually being designed to log and alert on attacker activity. Honeynets take the same concept but scale it up to emulate entire networks of legitimate-looking IT infrastructure. Honeytokens, on the other hand, are specific sequences of data embedded into production files or databases, that can then be used to trigger IDS alerts if the data is exfiltrated. These capabilities can provide economical detective controls for complex enterprises without having to incur the complexity and expense of trying to instrument the organization's full IT environment.
14. *Security Operations Center (SOC)* involves having a dedicated team and supporting infrastructure whose primary task is to monitor the organization's cybersecurity status, investigate security alerts, and follow up on security investigations. This capability is critically important to establishing an active defense, where the organization is responding to cyberattacks, repelling cyberattackers, and strengthening its defenses on an ongoing basis.

Incident Response

This functional area provides for the investigation, response, and recovery of incidents that are identified through monitoring of the organization's cyberdefenses. Incident response can be formal or informal, depending on the size of the organization and the magnitude of the incident. Incident response is most effective when the process is relatively formal, with structure, discipline, and a deliberate response. Before an incident occurs, formal communication channels and lines of authority should be clearly defined. Processes for assessing the situation need to be defined so the organization can understand when the situation is overwhelming its initial response. While incident response does not protect the organization from attacks, what it does do is give the organization the ability to respond to those attacks when they occur.

No matter how good or effective an organization's defenses are, incidents will occur.

Goal

The goal of this functional area is to provide for a timely response when security incidents are identified and incident response is warranted.

Objective

The overall objective of this functional area is to identify cyberattacks when they occur, mount a deliberate and appropriate response to the cyberattacks, and resolve and remediate the situation with a minimum of collateral damage.

Threat Vectors

Threat vectors addressed by the incident response function area include the following:

- Lack of an organization incident response process.
- Poor coordination between security staff and IT operations. This situation can result in operational staff not consulting security staff and inappropriately handling the incident without effectively repelling the cyberattack.
- The incident response process fails to feed indicators of compromise (IOCs) back to the monitoring and detection process. As a result, defenders falsely believe they have contained the incident, while the reality is that attackers continue to maintain their access into the organization's IT environment.
- The incident remediation process fails to adequately strengthen defenses that were breached. This situation allows attackers to re-enter the organization at a later date, potentially repeating the same or similar attack over and over again.
- Deliberate attackers leverage the incident response process during their attack to their advantage. For example, attackers force the organization into an incident response mode and then take advantage of the incident response process to trick defenders into disabling critical security controls.
- The incident remediation process fails to account for regulatory or legal requirements on reporting and disclosure. For example, the organization misses its regulatory requirements and potentially incurs financial, legal, or public relations penalties.

Representative Cybersecurity Capabilities

The capabilities in Figure 7.14 enable the organization to respond to incidents effectively and efficiently. Some of these capabilities are fundamentally procedural in nature. However, technologies can greatly assist with many of the steps involved in investigating, tracking, and repelling stealthy professional cyberattackers.

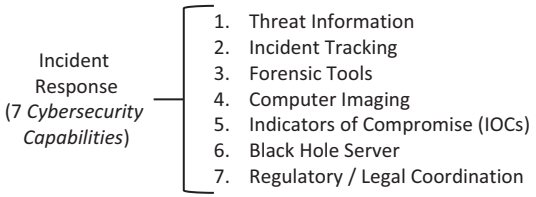


Figure 7.14: Representative cybersecurity capabilities for the *Incident Response* functional area.

These capabilities include the following:

1. *Threat Information* involves collecting information about the cyber threats against the organization, their *tools, techniques, and procedures* (TTPs), and cyberattack *indicators of compromise* (IOCs). This capability enables the organization to proactively detect cyberattacks, as well as to perform *cyber hunting* to search for and catch cyberattacks that may be in-progress.
2. *Incident Tracking* involves having a formal database or information system for tracking the cyber alerts that occur and the investigations triggered by those alerts. This capability helps to protect against important alerts "slipping through the cracks" as busy teams juggle priorities, and to help the cyber response teams to identify, triage, and respond to the cyber incidents that are of greatest importance.
3. *Forensic Tools* enable incident investigators to conduct cyber investigations in ways that preserve the evidence, support legal processes for conducting investigations, and provide a strong chain of custody for the evidence that is collected and analysis that is performed. This capability is important for cyber investigations that may lead to legal or criminal actions, or require eventual collaboration with law enforcement.
4. *Computer Imaging* involves being able to "snapshot" computer configurations, running programs, and system hard drives for later investigation. This capability is important to enable investigations to continue after affected systems have been remediated and re-imaged, to enable system operators to quickly re-image systems and restore service, and to enable collection of evidence for later legal consideration.
5. *Indicators of Compromise (IOCs)* involve collecting parameters that can be used to detect cyberattacks and attacker activity. These parameters may include computer addresses, internet domain names, network traffic patterns, or specific software code that can be used to identify an attack. This capability is used to "seed" detective controls with attack patterns to detect, and enables groups of organizations to rapidly share information about cyberattacks so that all may detect and defend, together.

6. *Black Hole Server* involves establishing the ability to intercept outbound or inbound malicious traffic, so it does not reach its intended destination. This capability may include replying back to the originator, so it appears to the attacker or the malware that the connection was successful.
7. *Regulatory/Legal Coordination* involves establishing formal processes for coordinating cyber incident investigations with interested external parties like regulators, business partners, and legal counsel. This capability includes policies, procedures, and oversight of the investigation process. When successfully performed, it ensures that the investigation satisfies its requirements for contractual, regulatory, and law enforcement purposes.

An effective cybersecurity program is not just about buying the latest technology and implementing it, nor is it just about people, procedures, or a series of checklists. An effective cybersecurity program involves balancing and integrating technology, processes, people, organization, budgets, and compliance requirements, in an efficient and cost-effective manner.

Chapter 8
Cybersecurity Operations

Once a cybersecurity program is in place with all of its technologies and capabilities, the task still remains to *operate* those cybersecurity capabilities and the controls they enable. *Cybersecurity operations* involves multiple processes, not the least of which is simply maintaining organization cybersecurity capabilities. An organization can have the best firewalls in the world, but if they are not configured to block potentially malicious network traffic, they are not doing any good. Similarly, an organization can lock down access to its most sensitive servers and databases, but if no one provisions access to those servers and databases, then the business is going to come to a grinding halt. It is critically important to execute organizational cybersecurity operations so that protections are maintained while also permitting the business to function.

As shown in Figure 8.1, *cybersecurity operations* – consisting of operational processes and their associated operational activities – leverage cybersecurity capabilities to support an organization's cyber protection and IT operations.

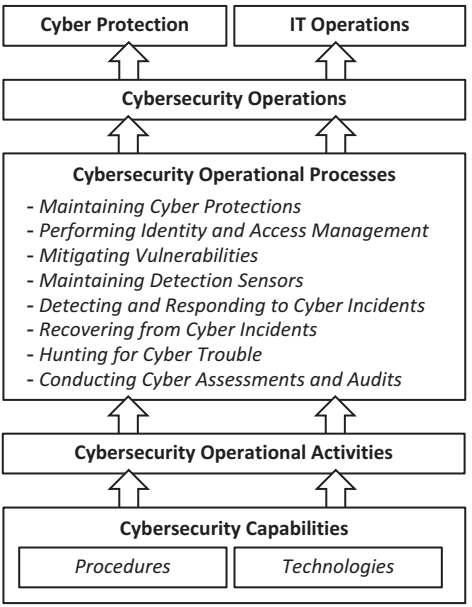


Figure 8.1: An organization's cybersecurity operational processes are built, in part, upon the cybersecurity capabilities needed to protect its core missions and business functions.

https://doi.org/10.1515/9781501506529-008

Cybersecurity personnel follow their operational processes to deliver cyber solutions to the business. At a high level, these processes can be described as follows:

- ***Maintaining Cyber Protections.*** Involves maintaining cybersecurity protections so that data, applications, servers, networks, and accounts are protected from inadvertent or malicious compromise, denial, or change.
- ***Performing Identity and Access Management.*** Involves configuring online accounts and identities for people, partners, and computer systems so they can be uniquely identified and granted permissions against internal IT systems.
- ***Mitigating Vulnerabilities.*** Involves identifying, tracking, and mitigating software IT system vulnerabilities in a timely fashion, particularly internet-facing application servers, critical infrastructure components (e.g., network switches, routers), and user endpoints.
- ***Maintaining Detection Sensors***. Involves maintaining applications, infrastructure, and other components involved in detecting cyberattack activities, so those components can detect cyberattacks when they occur.
- ***Detecting and Responding to Cyber Incidents.*** Involves actively detecting, investigating, and responding to cyber compromises when they occur to stop the attackers before significant damage can occur.
- ***Recovering from Cyber Incidents.*** Involves remediating cyber incidents so any damage that occurred is repaired and IT systems are restored back to their normal operations.
- ***Hunting for Cyber Trouble.*** Involves proactively searching the organization for signs of cyberattack activity, particularly cyberattacks that have breached the outer perimeter and have gotten into accounts, networks, servers, or endpoints.
- ***Conducting Cyber Assessments and Audits.*** Involves objectively evaluating the organization's cyberdefenses for the purpose of satisfying the organization's compliance obligations and progressively improving those cyberdefenses over time.

The following sections provide an overview of these cybersecurity operational processes, some of their most important operational activities, and how they might be implemented in an organization.

Maintaining Cyber Protections

The cybersecurity operational process of *maintaining cyber protections* involves maintaining cybersecurity protections so that data, applications, servers, networks,

and accounts are protected from inadvertent or malicious compromise, denial, or change. Figure 8.2 depicts some of this process's most important operational activities.

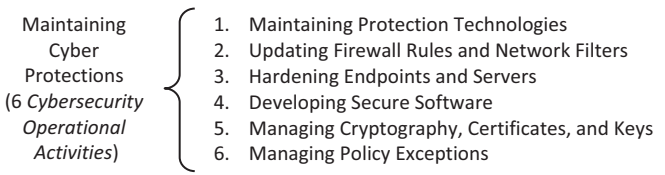


Figure 8.2: *Maintaining cyber protections* is necessary to help the organization keep pace with rapidly evolving malware and well-resourced cyberattackers.

Maintaining cyber protections includes maintaining, patching, and upgrading protection technologies installed at an organization. It also includes configuring those technologies to provide protections according to the organization's security policies. While it is nice to think that cyber protections can be configured once and then left alone, in practice, these technologies require constant maintenance and monitoring to keep them fully operational and their protections effective. Brief descriptions of these cybersecurity operational activities are as follows.

Maintaining Protection Technologies

The first step in this process is simply maintaining protection technologies in place. They must be configured, patched, updated, upgraded, and kept current with industry "best practices." Obsolete protection technologies must be identified and retired or replaced, as appropriate. An organization does not want its cyber protections to be the vulnerabilities that let the bad guys in!

Updating Firewall Rules and Network Filters

For organizations that operate their own networks, the perimeters of those networks require protection to block potentially malicious network traffic. To maintain this protection, firewall rules and filter configurations must be adjusted as components and applications are added or removed from the network environment, or when security requirements change.

Hardening Endpoints and Servers

Internet-connected computing devices – PCs, servers, mobile devices, and the internet of things (IoT) – are the front line of an organization's defenses. These systems should be "hardened" by turning off unnecessary features and configuring their security policies so they are less vulnerable to cyberattacks. In addition, this hardening configuration must be regularly updated as patches, applications, and operating system versions and features change.

Developing Secure Software

If an organization develops its own software, particularly if that software is customer-facing, then secure software development is going to be of critical importance. This process involves adding steps to the software development process to protect against software vulnerabilities. Developing secure software includes guarding against protocol issues, bad inputs from untrusted components, software corruption, data deletion, data modification, and data disclosure.

Managing Cryptography, Certificates, and Keys

Even if an organization does not do software development, it is likely using cryptographic techniques and technologies across the organization. Such techniques and technologies include certificates for servers and clients; protected protocols like Hypertext Transmission Protocol Secure (HTTPS) and Wi-Fi Protected Access (WPA); encryption for hard drives, data at rest, and data in motion; digital signatures for data validation; and authentication keys like passwords, biometrics, and hardware devices. All these components must be maintained and refreshed periodically to ensure they remain valid and up-to-date: rotate cryptographic key, renew certificates, and update cryptographic algorithms. Old, obsolete, or insecure cryptography must be retired, before it can pose a vulnerability.

Managing Policy Exceptions

Often overlooked, the policy exception process is foundational to a mature cybersecurity program. As the adage goes, "For every rule, there is an exception." Good risk management includes tracking those exceptions, their justifications, their mitigating controls, and their approvals. Good risk management also includes

periodically reviewing the approved exceptions, then extending or revoking those exceptions as appropriate to keep the organization's overall risk to an acceptable level.

Performing Identity and Access Management

The operational process of *performing identity and access management* involves configuring online accounts and identities for people, partners, and computer systems so they can be identified and granted permissions against internal IT systems. Figure 8.3 depicts some of the most important operational activities of this process.

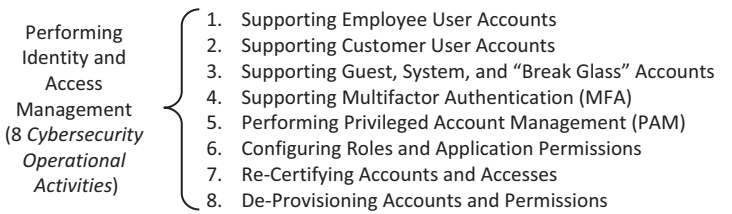


Figure 8.3: *Performing identity and access management* helps ensure only authorized people can access organization resources.

This process has become increasingly critical to organizational cybersecurity, as the traditional network-based perimeter has given way to virtual private networks (VPNs), cloud services, and third-party connections, all secured by digital online identities. In addition, increasing attacks against traditional username/password authentication have driven the need for multifactor authentication (MFA) and privileged account management (PAM). Finally, regulatory scrutiny and security concepts such as zero trust have driven increasing attention toward access management, as well as the close oversight of organization permissions governing who can access what, when they can access it, and where that access should be permitted. Brief descriptions of these cybersecurity operational activities are as follows.

Supporting Employee User Accounts

Identity and access management usually starts with employee user accounts. These are the accounts used by employees to authenticate to an organization's IT systems and perform their day-to-day jobs. Ideally, these accounts are automatically

created when employees are hired, and then removed when people leave the organization. Supporting these accounts includes providing for provisioning, de-provisioning, name changes, information updates, and password resets.

Supporting Customer User Accounts

For organizations delivering services across the internet, another type of account to consider is customer accounts. These accounts permit customers to identify themselves to organization systems and make purchases, exchange information, post to forums, or request support. These accounts are usually linked to customer relationship management systems, and require support for customer information changes, e-mail address updates, lost passwords, account lookups, billing, and payment changes.

Supporting Guest, System, and "Break Glass" Accounts

In addition to employee and customer accounts, there will likely be IT accounts for other parties, such as partners or contractors, guests, and application programs running over the network. Also, the organization will likely have "break glass" accounts that are used for emergency access to systems when failures or malfunctions have occurred. These accounts must also be managed, removed when no longer used, and should have their credentials changed or rotated on a regular basis.

Supporting Multifactor Authentication (MFA)

Multifactor authentication has become increasingly important for securing account access over the internet. It has also become common for protecting highly sensitive administration and financial accounts, even inside organizations' networks. However, it also increases support requirements, as MFA tokens (even virtual ones) must be inventoried, distributed, provisioned, and debugged when things go wrong.

Performing Privileged Account Management (PAM)

Similar to MFA, PAM has become an increasingly important identity and access management function. PAM systems must be maintained, and privileged accounts

must be checked out, checked in, and their passwords rotated on a regular basis. Also, audit logs must be checked to guard against signs of cyberattack, privilege escalation, or insider threat.

Configuring Roles and Application Permissions

Once accounts are in place for employees, customers, partners, and other users, the next step is managing roles and permissions for those users on the organization's IT systems. Roles are typically tied to the organization, reflecting functions like sales, customer support, or finance. Permissions are typically tied to the organization's IT systems, and tend to be application-specific. All of these roles and permissions must be configured and maintained on an ongoing basis, as the business and its supporting IT systems evolve and change. One technique for doing this is role-based access control (RBAC) which consists of separate sets of access control groups for organizational roles and application permissions.

Re-Certifying Accounts and Accesses

Once accounts, roles, and access permissions are in place, they should be revisited and re-certified on a regular schedule, such as quarterly or annually. Frequently, this re-certification is a regulatory requirement, and should be accompanied by artifacts documenting the re-certification and any changes resulting from it. The re-certification process should then drive the regular removal of permissions, roles, and accounts that are no longer needed by the organization or its people.

De-Provisioning Accounts and Permissions

Often directly coming from the re-certification process, de-provisioning is critically important to maintaining an organization's security posture on an ongoing basis. Ideally, de-provisioning should be automatic as roles, partners, users, and employees change or change positions. In practice, it tends to be far more complex and require multiple levels of checks, double-checks, escalations, and confirmations.

Mitigating Vulnerabilities

The operational process of *mitigating vulnerabilities* involves identifying and mitigating software vulnerabilities in IT systems, particularly internet-facing application servers, critical infrastructure components, and user endpoints. Figure 8.4 depicts some of this process's most important operational activities.

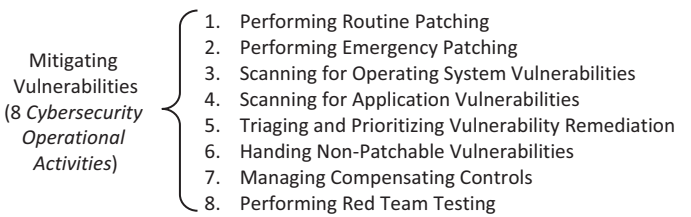


Figure 8.4: *Mitigating vulnerabilities* helps to reduce operational risks associated with known vulnerabilities.

This process is important because, unfortunately, modern software systems are mind-bogglingly complex. This complexity means bugs and vulnerabilities are rampant, malware to exploit those bugs and vulnerabilities is widespread, and patches to address problems are constantly being developed. Therefore, it is important for organizations to have a regular process for patching their software systems, scanning those software systems to ensure the latest patches have been installed, and also tracking and managing the risks associated with known vulnerabilities that, for various reasons, cannot be patched. Finally, these principles also mean that it is in an organization's interest to keep its software technologies and systems up-to-date. Where practical, obsolete software and systems should be phased out and retired, rather than keeping them in service past their prime. Particularly in IT, obsolete technologies tend to introduce security and operational risks that only increase over time. Brief descriptions of these cybersecurity operational activities are as follows.

Performing Routine Patching

The first step in the vulnerability management process is to perform "routine" patching. Routine patches are provided by software or device manufacturers to improve features, fix bugs, or otherwise maintain the proper operation of those systems. Ideally, system owners should patch their systems regularly, although in practice it is seldom that simple. Due to the complexity of modern, interconnected

networked systems, even basic patches can have unforeseen adverse impacts. To guard against these impacts, an organization should have patching processes that respect proper configuration control and change management, while also providing a streamlined path to production for keeping software components up-to-date.

Performing Emergency Patching

In addition to routine patching, an organization must have a process in place for performing emergency patching. Emergency patches are typically required for two reasons:

- An organization has an operational issue or outage that requires the deployment of a software patch to resolve.
- An organization has a cybersecurity vulnerability that is severe and requires the deployment of a software patch to resolve.

In both of these cases, the organization must have a process for adjudicating the risks involved in an emergency deployment, as well as a process for managing the testing and possible rollback of the deployment. Such adjudicating processes reduce the chance of things going wrong and address the operational problems in the event that the patch does go wrong.

Scanning for Operating System Vulnerabilities

Once patching has (or has not) been completed, the next step is to check for failures of the patching process. This checking usually involves scanning the IT environment for unpatched vulnerabilities using an open source or commercial vulnerability scanner. The result of the scan should be a list of vulnerabilities, along with scores for their relative importance. Cyberdefenders can use this information to identify which vulnerabilities require attention first, and which can perhaps wait until later.

Scanning for Application Vulnerabilities

Similar to scanning for missing operating system vulnerabilities, applications can be scanned as well. In addition to scanning commercial programs for missing patches, custom web-based applications can be scanned for application

vulnerabilities using non-credentialed and credentialed application scans.[1] These scans may also detect vulnerabilities stemming from certificate issues, cryptography problems, or application container mis-configurations. Advanced application scanners may also be able to detect issues with website cross-site scripting, weak input validation, embedded queries, or other application-specific problems.

Triaging and Prioritizing Vulnerability Remediation

Once vulnerabilities are identified, they should be triaged and prioritized based on *their risk to the organization*. Note that this vulnerability remediation is different from generic vulnerability criticality scores. In general, the risk to an organization is a function of the criticality of the vulnerability, along with the criticality of the vulnerable system.

- A critical vulnerability on a critical system should be of high importance.
- A critical vulnerability on a non-critical or non-production system may be of moderate or even low importance.
- A non-critical vulnerability on a critical system may be of moderate importance, or could even be of high importance, depending on the nature of the vulnerability.
- A non-critical vulnerability on a non-critical or non-production system may be of such low importance that it will not actually be addressed – so long as the organization does not let such non-production systems become a foothold for attacks.

Handling Non-Patchable Vulnerabilities

In practice, many types of vulnerabilities may not be patchable. These may be vulnerabilities in systems that cannot be patched, or for which patches are not available (old Android devices are a good example of this situation). Many older systems are vulnerable and will never get patches to address those vulnerabilities. In these cases, the systems, the vulnerabilities, the potential consequences of compromise, and the resulting business risks should be tracked, along with short- and long-term plans for managing those risks.

---

1 Non-credentialed scanning does not use system credentials to provide a vulnerability assessment from a cyberattacker's viewpoint. Credentialed scanning uses system credentials to provide a vulnerability assessment from an organization's viewpoint, which can include a list of required patches and misconfigurations.

Managing Compensating Controls

Where systems are vulnerable and cannot be patched, the organization should track the risks and consider compensating controls. Main types of compensating controls include:

- Isolating vulnerable systems to make them more difficult to attack and to reduce the attack surface.
- Performing active monitoring and detection around such systems to be able to proactively detect and respond to compromises should they occur.
- Engineering systems to limit the damage of a compromise, should one occur.

In many cases, an organization may want to use a combination of two or even all three types of compensating controls to manage the risk of vulnerable systems.

Performing Red Team Testing

Red team testing can complement vulnerability scanning and vulnerability management by looking at vulnerabilities not only in terms of individual systems, but in terms of the organization's entire IT environment as a whole. Among other objectives, red team testing is intended to address the following central question:

- *Can attackers – or at least simulated attackers – exploit enough vulnerabilities or other security issues to successfully penetrate the organization's perimeter, establish a foothold inside the network, perform command-and-control, and then move laterally and escalate privileges to get to their target?*

If the answer to this central question is "yes," then the red team test will likely result in recommendations for additional security work.

Maintaining Detection Sensors

The operational process of *maintaining detection sensors* involves maintaining applications, infrastructure, and other components involved in detecting cyberattack activities, so those components can detect cyberattacks when they occur. Figure 8.5 depicts some of this process's most important operational activities.

For a long time, detection capabilities were largely ignored in favor of preventive controls focused on blocking potentially malicious activity. However, the advanced persistent threat (APT) cyberattacks and breaches of the 2010s showed

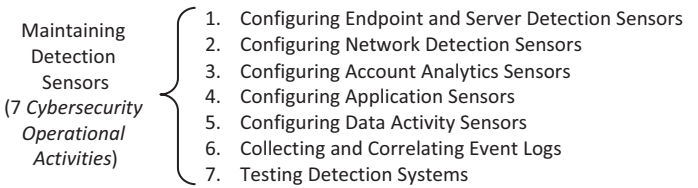


Figure 8.5: *Maintaining detection sensors* helps prevent cyberattackers from operating undetected and reduces the risk of them gaining control of user accounts and organization systems.

that even with good cyber prevention in place, some attacks are bound to get through. Modern IT organizations cannot ignore the power of detection and timely response. But before an organization can achieve good detection, it must have good visibility, which requires sensors on its endpoints, networks, accounts, applications, and data. These sensors must then be configured, monitored, and tested for effectiveness. Brief descriptions of these cybersecurity operational activities are as follows.

Configuring Endpoint and Server Detection Sensors

The first detection sensors to consider are the managed endpoints and servers of an organization. The most common sensor source of data is anti-virus software, but other components – such as advanced malware detection, endpoint firewalls, user authentications, and system logs – can serve as detection sensors as well. Collection of endpoint and server logs, in particular, can be extremely helpful for gaining visibility across an organization's IT systems. This visibility can then be used to track potential attacker activities and behaviors, not to mention insider threats.

Configuring Network Detection Sensors

In addition to monitoring endpoints and servers, network detection sensors can provide visibility into potentially malicious network traffic. This monitoring includes network traffic into the organization's network, out of the organization's network, and within the network itself. In particular, traffic across network boundaries – such as between user spaces and data centers, between data center sites, or among applications – can be monitored to detect many different types of attack behaviors and malicious software communication patterns.

Configuring Account Analytics Sensors

Another useful source of insight into an organization and possible malicious activity is account activity. This activity can include basic activity like system log-ins, log-offs, and failed authentication attempts. It can also include more advanced analytics like authentication patterns, time-of-day analysis, geographic patterns, or even keyboard keystroke patterns (different people might type the same password in different ways). While advanced analytics are labor intensive to tune and prone to false positives, they can be extremely helpful in detecting account credential abuse and even insider threat activity.

Configuring Application Sensors

Above and beyond account analytics, additional visibility can be gleaned from logs and sensors tied to specific applications. These sensors may be as simple as alerts from e-mail gateways to indicate malicious e-mails, or to enable investigation of e-mails that are let through but later turn out to be malicious. The sensors may also include sophisticated advanced analytics searching for specific behavioral patterns. These analytics can then be applied to organization applications for sales tracking, customer resource management, organization resource planning, financial reporting, or collaboration. These sensor configurations tend to be very specialized and tied to the features and data structures of the application to be monitored. However, for financial or transaction processing systems handling millions – or even billions – of dollars, the investment can be worthwhile.

Configuring Data Activity Sensors

Another important source of visibility into an organization's cyber environment is the data itself. While data may be located in many places – file shares, applications, databases, data repositories, and backups – accesses to that data can be logged, analyzed, and monitored for anomalies. While these logs are most often used to support investigations rather than detection, modern analytics and artificial intelligence tools are becoming increasingly capable of processing data activity logs to alert on potentially malicious activities, and with ever-increasing levels of fidelity.

Collecting and Correlating Event Logs

An important part of achieving effective detection is bringing the logs involved together to achieve a single, central picture of cybersecurity activity. A key part of this cybersecurity operational protection activity is *correlation* – so that timelines can be unified, IP addresses can be resolved into host names, network address translation can be reversed, and account IDs can be resolved into usernames – to make it easier to understand what is going on in the logs. With processed, consolidated, and correlated event logs, analysts can follow the logs to trace attacker activity across the organization, as well as its systems, networks, and accounts.

Testing Detection Systems

How does an organization know that its detection system is working, if the organization does not test it? A critical step in building an effective detection platform is to regularly test the platform and its sensors using simulated attacker activity. Testing can involve the following actions:

- Injecting malware onto an endpoint to see if the endpoint detection works.
- Sending malicious network traffic over the network to see if network detection works.
- Exfiltrating data from an application or database to see if data protection sensors work.
- Having a red team do a simulated attack, and seeing if your analysts can detect the attack or reconstruct its activities from the logs.

Organizations should perform regular testing of their detective controls and detection sensors to verify their proper operation and to detect if preventive or detective controls have failed, have been disabled, or are malfunctioning.

Detection cannot be successful long-term if it is not regularly tested.

Detecting and Responding to Cyber Incidents

The operational process of *detecting and responding to cyber incidents* involves actively detecting, investigating, and responding to cyber compromises when they occur. The goal of this response, ideally, is to stop the attackers before significant

damage can occur. Figure 8.6 depicts some of this process's most important operational activities.

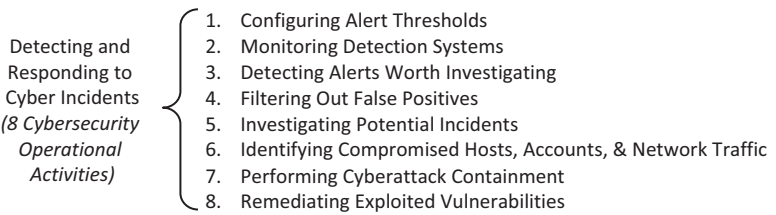


Figure 8.6: *Detecting and responding to cyber incidents* involves (1) "tuning" organization cybersecurity monitoring systems to identify real security incidents, (2) investigating those incidents to find cyberintruders, and (3) repelling cyberintruders in such a way that it will be hard for them to get back into the organization again.

This process is probably the *single most important operational process* in the modern cybersecurity ecosystem. Without this process, even the most diligently protected IT systems are bound to eventually become compromised. From that initial compromise, deliberate attackers will likely be able to eventually move laterally, escalate privileges, and do damage to even the best-protected IT systems. By detecting and responding to these attacks after they start, but before they can fully succeed, organizations can sharply reduce the amount of damage that is done. While it may not prevent some damage from occurring, detection and response activities should help to prevent the cyber worst-case scenarios from coming to pass. Brief descriptions of these cybersecurity operational activities are as follows.

Configuring Alert Thresholds

The first step in detecting and responding to cyber incidents is to have alerting systems in place that can "raise the alarm" when something happens. Some tools, like anti-virus, are straightforward to configure and may warrant investigation almost every time they alarm. Other detection systems, like network traffic monitors or behavioral analytics, may involve more technical and delicate tuning processes. The more advanced detection systems will most likely require more constant configuration and tuning to keep them effective and filter out false positives.

Monitoring Detection Systems

Once detection systems have been tuned, the next step is to watch out for alarms that occur.

Warning: Too many organizations miss this step!

In particular, if detection systems are not integrated together, or alerts consolidated, then monitoring may involve looking at multiple screens of multiple systems to check for events of concern or alarms needing action. Or it may involve searching log files for particular patterns of concern. To be successful here, organizations must *Automate, Automate, Automate!* Configure detection systems to send cyber personnel a daily e-mail, or write scripts to consolidate alerts from multiple consoles into a single, unified view. The more places the cyber team has to look for important cyber alerts, the more likely it is that the team will miss something important when it does occur.

Detecting Alerts Worth Investigating

Once an organization is actually monitoring its detection systems, the next step is to figure out which alerts warrant investigation. Alerts like anti-virus warnings or network malware alerts are usually pretty straightforward, but alerts from privileged account monitoring or user activity sensors may make it harder to determine which ones warrant investigation. Advanced alerting, in particular, may be "noisy" and generate many alerts that are not of immediate concern. Such alerts may be helpful to establish context for other alerts, or only need to be investigated if something else occurs at the same time. Organizations should have guidelines on what should be investigated and what can be safely ignored, and under what circumstances.

Filtering Out False Positives

The more "noise" detection and alerting systems make, the harder it will be to identify which alerts actually warrant taking action. When only a couple of alerts are occurring each day, it may be okay for most of them to not require action. On the other hand, once a single person has to look at hundreds or thousands of alerts each day, figuring out which ones to act on becomes much

more challenging, and the odds of missing something important go up dramatically. At this point, additional work should be done to filter out these false positives, or to somehow highlight in the data those alerts most likely to warrant investigation.

Investigating Potential Incidents

Once an organization identifies alerts that are of interest, the next step is to investigate those alerts to understand what is going on. This investigation can involve pulling a variety of logs from endpoints, network traffic, and account activity. From those logs, the organization may find signs of malware installed on endpoints, malicious network communications, and account compromise or abuse. In its investigation, the organization will be figuring out the tools, techniques, and procedures (TTPs) used by the attackers, along with indicators of compromise (IOCs) to find attacker activities within the organization's IT environment.

Identifying Compromised Hosts, Accounts, and Network Traffic

As an organization investigates the attacker's TTPs and IOCs regarding the attack that is in progress, it should keep track of the hosts, accounts, and network traffic patterns involved in the cyberattack, along with signs of malicious software or malware. In a large environment, this investigation process can span large numbers of computers, devices, accounts, tools, and network traffic patterns. Each time new information is revealed, the organization will want to scan its entire IT environment for those patterns until it has an understanding of the full scope of the cyberattack. The longer it has been since the attack began, the wider the span of the compromise may be.

Performing Cyberattack Containment

Once an organization has a handle on the cyberattack, the cyberattackers, and the hosts, accounts, and network traffic patterns involved in the cyberattack, it will want to perform containment. Containment should stop the spread of the cyberattack and deny the attackers access to the IT environment so the organization can do cleanup and remediation. *It is important to not perform containment prematurely, as tipping off the attackers can cause them to switch techniques or tools and become "invisible" within the organization's IT*

environment. One technique for performing containment is to disconnect from the internet entirely, and then remediate hosts and accounts while disconnected to prevent the attackers from counterattacking while the cleanup is underway. Note that containment does not require that everything be restored to operation, just that the attackers be stopped and contained. Another technique is to put sensors in place as part of remediation so that subsequent attacker activities – such as attempting to use a previously compromised account – set off alarms for follow-up investigation.

Remediating Exploited Vulnerabilities

In conjunction with the containment effort, an organization will also want to remediate the vulnerabilities the attackers exploited to get into the IT environment in the first place. If the environment is not hardened against subsequent attacks, it is easy to get into a game of "whack-a-mole" with determined attackers who keep coming back over and over again. By remediating the exploited vulnerabilities, as well as other vulnerabilities that become apparent during the investigation process, the organization can reduce its risk of subsequent re-infection and deter the attackers from continuing their attack or later trying to come back again.

Recovering from Cyber Incidents

The operational process of *recovering from cyber incidents* involves remediating cyber incidents so that the damage that occurred is repaired and IT systems are restored back to their normal operations. Figure 8.7 depicts some of this process's most important operational activities.

This process may be as simple as running an antivirus "clean-up" command, or it may involve dramatic actions like reinstalling operating systems and applications, or globally changing all passwords for the entire organization. It may also involve recovering or re-constructing deleted or damaged data, or the applications that handle that data. Frequently, it will involve dealing with customers, partners, or regulators regarding breached, damaged, or deleted data records. Depending on the magnitude of the breach, public relations and legal activity may also be involved. At the end of the recovery, the organization will likely also want to strengthen its cyber defenses to "ensure this situation never happens again," or at least to reduce the likelihood or the impact of similar incidents in the future. Brief descriptions of these cybersecurity operational activities are as follows.

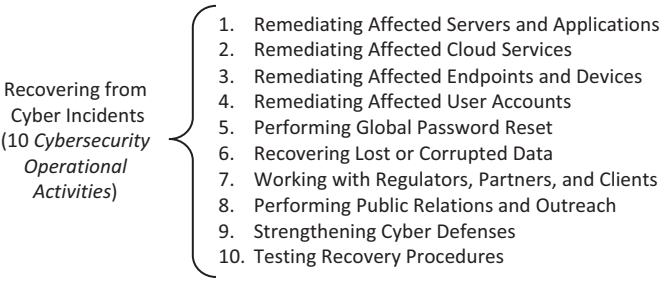


Figure 8.7: *Recovering from cyber incidents* involves (1) restoring the organization to normal operations, (2) working with customers, partners, or regulators regarding the breach, and (3) strengthening cyber defenses.

Remediating Affected Servers and Applications

The first step in the recovery process is usually to restore servers and service applications affected by the cyberattack. For example, if the attack affects an organization's public website, internet-facing e-mail, or production IT systems, getting those systems restored is probably going to be a top priority. This recovery may involve rebuilding servers, reinstalling applications, or restoring data from backups. If data or transactions were corrupted, they may have to be restored based on log records, or even manually reconstructed. Multiple steps may be involved in the overall remediation effort – including the use of backup systems, interim capabilities, or external services – while primary servers and applications are being restored.

Remediating Affected Cloud Services

Like on-premise IT, cloud services may also be affected by compromise and require remediation. Cloud service remediation is going to depend greatly on the type of cloud services, the capabilities of the service provider, and the extent of the compromise. Most often, cloud compromises involve some form of credential misuse, with backup and restore functions remaining available to support the restoration process. In other circumstances, the breach may extend into, or lie within, the cloud provider itself. In these cases, the organization may have to change cloud providers, or at least engage contingency services to quickly restore operations.

Remediating Affected Endpoints and Devices

In addition to servers and cloud services, user endpoints and other devices may also be compromised and require remediation. Generally, the "safest" approach here is to reimage these devices with known, configuration-controlled operating system software and applications, and then restore user data from backups. Sometimes, remediation may not be possible and equipment has to be replaced altogether. This situation can occur with network-connected devices where the firmware has been corrupted, or if low-level device drivers are used to cause hardware damage. In other cases, less dramatic actions may be sufficient. Such actions can include manually removing malware files or simply updating system configurations to remove the compromise. In all of these cases, the goal is to restore operations while removing the vulnerabilities and tools that were used by the attackers to perpetuate their attack.

Remediating Affected User Accounts

User accounts will likely also be affected by the attack and require remediation. The affected accounts may include employee and partner accounts, as well as system accounts used for inter-application communications and privileged systems administration functions. In almost all cases, "remediating" user accounts involves changing their passwords and updating any copies of those passwords that are stored in configuration files or password managers. In some cases, it may include changing account names, or even deleting accounts and then reprovisioning them from scratch. Remediation may also include placing additional monitoring around sensitive user accounts to catch potential attempts at future compromise or abuse.

Performing Global Password Reset

In more severe cyberattacks, attackers may compromise an organization's authentication infrastructure, enterprise directory, or password repositories. In these cases, the attackers may gain the ability to read the password of every user in the organization or may attempt to "crack" the cryptography protecting those passwords. In these cases, it may be prudent for the organization to do a global password reset, and change the passwords of all of its users, all at once. While this reset sounds straightforward in principle, global password resets are surprisingly difficult to execute in practice. In particular, privileged system account passwords

may be almost impossible to change without rebuilding major parts of an organization's IT environment. When doing a global password reset, the organization should do what it can to change passwords across the board, and then use account monitoring to protect those accounts that are most critical or whose passwords cannot be easily updated.

Recovering Lost or Corrupted Data

One cannot overstate the importance of good data backups and good cryptographic key management for encrypted data. Frequently, data will be encrypted multiple times over, with encryption applied at the hardware, operating system, application, database, and even user levels. All of the keys used for this encryption must be managed and available, if backed up data is to be recoverable and usable. Similarly, the most important data should be backed up multiple times and then encrypted using separate encryption systems. The goal needs to be to avoid making backups or encryption into "single points of failure" that could result in catastrophic losses of critical business data, should something go wrong with the data recovery process. In addition, the organization will need to have robust data and transaction log records to enable the reconstruction of data that may have become corrupted or deleted in an attack.

Working with Regulators, Partners, and Clients

Once an organization knows what data is affected by a cyberattack, it will need to consider the regulatory and contractual obligations associated with that data.

- *Is data governed by privacy regulations like HIPAA or industry standards like PCI DSS?*
- *Are there regulator or public disclosure requirements, as with GDPR?*[2]
- *Are there contractual obligations with partners or clients that need to be considered?*

The organization's legal team will need to know these facts so it can look at what requirements apply to the situation, and what actions the organization is obligated to take. Similarly, the organization may need to work with business

2 Health Insurance Portability and Accountability Act (HIPAA); Payment Card Industry Data Security Standard (PCI DSS); and General Data Protection Regulation (GDPR).

partners and clients to address effects on their businesses and the organization's business relationships with them. Once again, the organization's legal team will likely have guidance on what the organization can do, what it can't do, and what it must do.

Performing Public Relations and Outreach

If the cyberattack involves regulated data (particularly healthcare, privacy, financial, or credit card data), then public disclosure of the breach will likely be necessary and appropriate. This outreach may be as simple as posting a public announcement on a website, or it may be as involved as offering credit protection, operating call centers, or dealing with class action lawsuits. In all of these cases, there will be messaging – public announcements, postings, and comments by executives – that will need to be carefully crafted. These messages may need to comply with certain disclosure requirements while also being careful to not make an already bad situation even worse. Unfortunately, saying too little, saying too much, or saying "the wrong things" can all make the situation worse, so messaging must be carefully crafted and carefully delivered. An organization should not be shy about engaging outside experts, even if it already has communications expertise in-house. There is a lot at stake, and missteps can have huge consequences.

Strengthening Cyber Defenses

Once the situation has been contained, the cyberattack remediated, compliance requirements satisfied, and public outreach conducted, there is the question of ensuring the situation "will never happen again." While no cyberdefense can possibly be perfect, cyber breaches frequently lead to an increase in cybersecurity as a business priority, with all of the attendant resources and management attention. This situation can become an opportunity to invest in some of those cyber improvements that the cyber department may have wanted for a long time, but been unable to afford. Such investments may include a re-design of internal networks to provide more in-depth defense, deployment of multifactor authentication, improvements in log aggregation and monitoring, or prepositioning of forensic investigation and cyber recovery tools. The aftermath of a cyber incident can be a good opportunity to revisit the organization's cyber strategy, cyber resources, and cyber priorities, with an eye toward making some changes and improvements.

Testing Recovery Procedures

Finally, even if a cyber incident or crisis has not occurred, it is *always* a good time to review and test an organization's cyber incident recovery procedures. This testing can be as thorough as doing a full recovery exercise at the organization's disaster recovery location. Or it can be as simple as doing a tabletop exercise via teleconference. The important part is for personnel to think through the incident and recovery processes, the steps they would take, and the resources they would need. One approach is to do monthly or quarterly drills, and then have an annual exercise that involves more resources or engages outside consultants for a realistic scenario. In these exercises, the organization should make sure its employees know what needs to happen, who needs to do what, and how pre-preparation can make things easier ahead of the crisis situation. An organization does not want to wait for a real crisis to find out that critical passwords, cryptographic keys, system documentation, or other resources are all contained somewhere that got wiped out by the attackers, five minutes after the initial breach occurred.

Hunting for Cyber Trouble

The operational process of *hunting for cyber trouble* involves proactively searching the organization for signs of cyberattack activity, particularly cyberattacks that have breached the outer perimeter and gotten into accounts, networks, servers, and endpoints without being otherwise detected. Figure 8.8 depicts some of this process's most important operational activities.

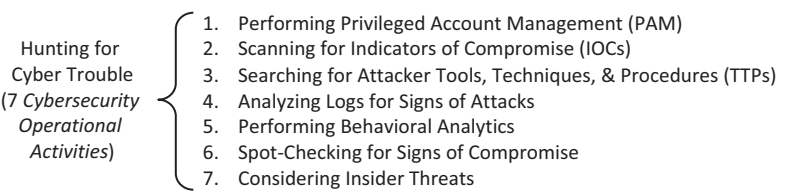


Figure 8.8: *Hunting for cyber trouble* involves analyzing computers, network accounts, network connections to identify malware, resources, and techniques used by cyberattackers to attack the organization.

In most of the high-profile breaches of the 2010s, attackers were inside the victim's IT systems for hours, days, weeks, or even months before their attacks were fully carried out. This period, known as "dwell time," is the time during which

the attackers are establishing themselves within the victim's IT environment, reconnoitering networks and systems, moving laterally, and escalating privileges to get access to their ultimate objective. During this dwell time period, defenders have an opportunity to catch and repel the attack before much real damage has been done. By hunting for cyberattackers dwelling in its IT systems, the organization has a tremendous opportunity to dramatically reduce its cyber risk before the cyber alarms go off. Brief descriptions of these cybersecurity operational activities are as follows.

Performing Privileged Account Management (PAM)

In a majority of cyberattacks, attackers seek to get access to privileged accounts belonging to system administrators, application administrators, and domain administrators. With these privileged accounts, the attackers can log in to large numbers of computers, applications, servers, databases, or other systems underpinning an organization's IT infrastructure. PAM can protect these accounts by automatically managing their passwords and then enforcing access to those passwords from a "vault" or other hardened IT system. When properly implemented, PAM makes it very difficult for attackers to move around the IT infrastructure without having to get into the PAM system first. This *single point of security* can then be hardened to make it difficult to attack, as well as to detect signs of attempted attacks. By monitoring and reviewing PAM logs, defenders may find signs of cyberattacks while those attacks are in progress, but before the attackers can get past the PAM line of defense.

Scanning for Indicators of Compromise (IOCs)

IOCs are patterns in user activity, data activity, file contents, network traffic, or just about anything else that can be found in an IT system indicating, with a high level of confidence, potential attacker activity. Sometimes, industry cyber organizations (e.g., governments, commercial organizations, and open sources) publish IOCs for known cyberattacks, so that organizations can scan their environment for signs of those attacks. Other times, organizations can create their own IOCs from published best practices, or simply using common sense, based on how their IT environments work. Ideally, an organization should have monitoring in place to automatically raise alarms on the most common IOCs, as well as those provided to the organization through automated threat intelligence feeds. In addition, the organization can also search its systems for just about

any IOCs at any time. To perform hunting with IOCs, an organization can simply pick a couple of IOCs, and search its IT environment logs for signs of those IOCs over the preceding day, week, or month. Or the organization can perform a known IOC to see if it is detected by detective controls and alerted on, or at least logged. All of these actions can catch potential attacker activity that is occurring within the organization. In addition, if they do not catch any attacker activity, they can give the organization confidence that its defenses are operational and working as they should be.

Searching for Attacker Tools, Techniques, and Procedures (TTPs)

While IOCs indicate the trails left by cyberattacks as they occur, TTPs are the indicators that the attackers bring with them to the attack. In addition to malware, cyberattackers may use the tools already in an organization's IT environment, like Secure Shell (SSH), Microsoft's PowerShell, File Transfer Protocol (FTP) and Network File System (NFS). Other tools commonly used by cyberattackers include Microsoft's PsExec and Windows Management Infrastructure (WMI). Both of these are tools that enable remote connections and malware distribution. However, cyberattacks are different from regular system management, and cyberattackers will likely use these tools in ways (or from locations) that do not match legitimate systems administration. By characterizing the differences between malicious and legitimate systems administration activity, the organization can search its environment for abuse of these administrative tools, just as it can search for IOCs. An organization can also search for attacker procedures, such as using the commands "whoami," "ping," and "netcat"[3] together to perform reconnaissance. Many of an organization's TTP searches can be automated, resulting in powerful detective controls.

Analyzing Logs for Signs of Attacks

In addition to privileged account management (PAM) systems, IOCs, and TTPs, an organization can also look in its system logs for signs of attacks that are being attempted or, worse, that have already succeeded. While IOCs and TTPs

3 "Whoami" is a command that displays the domain and username of the current user; "píng" is a command that verifies a computer can communicate over the network with another device or computer; "netcat" is a network utility that can read from or write to network connections using transmission control protocol (TCP) or user datagram protocol (UDP).

involve looking for attacker and malware patterns that are well known, log analysis involves looking for patterns that are specific to an organization's IT environment. An organization may consider the following questions:

- *What might attackers do that is specific to the organization's IT environment, but still different from legitimate activity?*
- *Would attackers go after a specific server, client, or user account?*
- *Would attackers come in through a specific network gateway, or have to traverse a specific network interface?*

Log analysis involves identifying patterns that might be indicative of attacker behavior in an organization's environment, and then searching its logs for those patterns. An organization can do this log analysis as a one-off activity, or it can automate the analysis into scripts that run regularly – say, hourly, daily, or monthly – and then monitor those scripts for alerts. Ideally, this log analysis will evolve into detective controls that can catch attacker behavior in an organization's environment, preferably with a low number of false positives.

Performing Behavioral Analytics

Once an organization has visibility inside its logs, there is no limit to how much it can analyze them. One approach is to use machine learning or artificial intelligence technologies to perform behavioral analytics, particularly on logs that capture human activities. These algorithms work by establishing "baselines" of behaviors and then flagging activity that is "inconsistent" with those baselines. The thresholds for "inconsistent" are dynamically set by the analytics engine, perhaps using proprietary algorithms, or perhaps using scoring mechanisms that an organization may be able to help tune. Either way, the engine will use its "intelligence" to find patterns that may be of interest. While these systems can be hard to tune and may have lots of false positives, they can also find proverbial "needles in haystacks" of log data that the organization never would have found on its own.

Spot-Checking for Signs of Compromise

Another cyber-hunting technique involves spot-checking the IT environment for signs of compromise. These signs can be known IOCs or TTPs, or can be taken from the organization's own IT systems. An organization may consider the following questions when spot-checking its systems:

- *Is there evidence of administrator credential hashes cached on systems not used for systems administration?*
- *Are there copies of customer database files not residing where they should be?*
- *Does the organization see social security numbers, credit card numbers, or other sensitive data going across network boundaries?*
- *Are there unexpected changes occurring in the IT environment to sensitive files, user accounts, or permissions groups?*

Also, an organization can look at operational performance:

- *Are there signs of high network traffic when there shouldn't be, or high CPU usage on systems that should be idle?*

At any time, an organization can spot-check for these types of signs. In addition, an organization can turn these checks into automated alerts using scripting, tools, or analytics, which is even more powerful because it will be constantly running.

Considering Insider Threats

Another factor to consider is the "insider threat." Insiders are people who have legitimate access to organization IT systems, and may even have elevated privileges to access, configure, or administer those systems. While 99% of the time, these people are honest, trustworthy employees or partners who only want what is best for the organization, the fact is that a small percentage of the time things go awry. Someone may give into temptation or be persuaded by an outsider to betray the trust that has been afforded to them. Also, they may make simple mistakes through error, carelessness, or negligence. In all of these cases, significant damage can occur due to insiders' positions within the organization and its IT systems. Often times, insider behavior will not be blocked or detected by traditional cybersecurity controls. Some insider behaviors can only be caught by advanced controls, checking of logs, behavioral analytics, separation of duties, or two-party controls. And even then, it is often difficult.

Conducting Cyber Assessments and Audits

The operational process of *conducting cyber assessments and audits* involves objectively evaluating an organization's cyberdefenses for the purpose of satisfying the organization's compliance obligations and progressively improving those

cyberdefenses over time. Figure 8.9 depicts some of this process's most important operational activities.

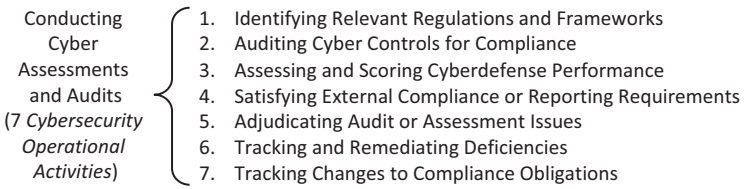


Figure 8.9: *Conducting cyber assessments and audits* involves: (1) identifying applicable frameworks and standards, (2) assessing or auditing organization operations against those cybersecurity frameworks, (3) identifying areas for improvement, and (4) remediating identified deficiencies.

This process is critically important to organizations that are required to comply with regulations pertaining to data protection or privacy. And who isn't! HIPAA, SOX, GDPR, CCPA, FISMA,[4] and a slew of other regulations all pertain to protecting regulated data like personal information, healthcare information, credit cards, and bank accounts. Few organizations *don't* handle such data in some way or another, and most organizations have copies of such data in places their management would never conceive. Unfortunately, when a single computer can hold millions of pages of information, and the entire *Encyclopedia Britannica* can fit onto a single digital versatile disk (DVD), it becomes very hard to control how data gets copied and disseminated.

Cyber assessments and audits serve to evaluate the controls around the organization's most sensitive data and IT systems. They also serve to provide actionable information on how well those controls are working, and how those controls might be improved. Armed with this information, an organization's auditors, executives, and leadership can strategically manage its cyber posture and cyber priorities. Cyber assessments and audits involve a number of operational activities to conduct the assessments or audits, collect the results of the assessments or audits, and then to remediate and address the deficiencies that are found by the assessments or audits. Brief descriptions of these cybersecurity operational activities are as follows.

4 Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and U.S. Federal Information Security Management Act (FISMA).

Identifying Relevant Regulations and Frameworks

The first activity in this process is to identify the regulations and frameworks that pertain to an organization. For regulations, this information will likely come from the organization's legal department, compliance department, or external financial auditors. The information may also come from industry associations related to the organization's area of industry, such as credit card processing, financial activity, medical information, or critical infrastructure. For frameworks, an organization has considerably more flexibility, as the cyber frameworks it uses to evaluate its operations are largely up to the organization. Common frameworks include the NIST Cyber Security Framework (CSF), the International Organization for Standardization (ISO) 27000 family of standards, and the Center for Internet Security (CIS) 20 Critical Controls. Each framework offers different areas of focus and priority for cybersecurity, and while none of them is "a single truth" on how to do cybersecurity "perfectly," all of them will provide the organization with useful insight into areas where its cyberdefenses can potentially be improved.

Auditing Cyber Controls for Compliance

Once an organization selects the frameworks for a "compliance audit," the auditors can evaluate organizational cyberdefenses for compliance with those frameworks. Generally, when conducting an audit, the objective is to make an *assertion of compliance* with the applicable standard: either the organization meets the standard, or it does not. So audit frameworks tend to be organized around binary statements of what cyberdefenses do, or do not do. Some examples of audit requirements include:

- *Do organization networks have firewalls protecting them?*
- *Does the organization monitor user account behavior?*
- *Does the organization detect sensitive data being sent out of its systems?*

Auditors will evaluate such statements, and then look at the organization's IT environment to determine if the statements' requirements are being met, or not.

Assessing and Scoring Cyberdefense Performance

Similarly, once frameworks for an organization's "performance assessment" are selected, the assessors can evaluate the organization's cyberdefenses against

those frameworks. Unlike audits, assessments cannot produce assertions of compliance. What assessments *can* do is evaluate the quality of the organization's cyber controls. In general, assessments score cybersecurity controls on a scale of 0% to 100%, 1 to 10, or maturity ratings on a scale of 1 to 5, with higher numbers indicating better security.[5] This information can then be used to quantitatively measure cyberdefense performance, track that performance over time, and compare that performance with peers and industry standards. This information can be helpful in determining if the organization's cyberdefenses are "good enough" and "in-line with industry norms," as well as identifying areas for potential improvements.

Satisfying External Compliance or Reporting Requirements

Once an organization audits or assesses its cyberdefenses against applicable regulations or frameworks, it can use that information to satisfy external compliance or reporting obligations. Regulators, insurers, and customers may all be interested in an organization's cybersecurity status information, as embodied by these audits or assessments. Sometimes, they may be interested in a summary of the results, or just an excerpt covering a particular area. Other times, they may be interested in the full result – it depends. In all cases, an organization should look at its audit and assessment results carefully, as they may contain a detailed analysis of its cyberdefense effectiveness and vulnerabilities. In some cases, these reports may contain enough detail to enable a cyberattacker to penetrate organization defenses. Regardless, audit and assessment details should be closely guarded and only shared with others when appropriate or necessary.

Adjudicating Audit or Assessment Issues

In evaluating audit and assessment results, there will likely be "judgment calls" in terms of compliance or non-compliance. Unfortunately, cybersecurity compliance is seldom a clear-cut "yes or no" determination. Where differences of opinion occur between an organization and its auditors or assessors, it may need to

5 For example, the US Department of Defense defines the following Cybersecurity Maturity Model Certification (CMMC) levels of cybersecurity practices: (1) CMMC Level 1-Basic Cyber Hygiene, (2) CMMC Level 2-Intermediate Cyber Hygiene, (3) CMMC Level 3-Good Cyber Hygiene, (4) CMMC Level 4- Proactive, and (5) CMMC Level 5-Advanced/Progressive.

document those differences, as well as the arguments for and against each side's positions on the matter. An organization may also want to document when an audit or assessment reveals an issue, and the organization's management chooses not to address the issue, or "accepts the risk" associated with the issue. Not every risk can be economically handled, and some level of judgment and risk tolerance is going to be necessary.

Tracking and Remediating Deficiencies

Similarly, audits and assessments are going to identify issues that should be addressed, or deficiencies that should be remediated. These issues should be formally tracked, assigned to appropriate parties for action, and tracked to completion. Even issues that are risk-accepted through adjudication should be tracked to ensure that they do not get worse or have unintended consequences. Deficiencies found in one audit or assessment should be brought to subsequent audits or assessments to identify trends and recurring issues. Areas of recurring deficiencies should be considered for management focus, investment, or operational improvements.

Tracking Changes to Compliance Obligations

An organization should monitor its compliance obligations and the regulatory frameworks and standards that apply to its business, as they can change in multiple ways. First, new standards or frameworks can be applied to the organization, or can become necessary due to changes in the business or its relationships. Second, the standards or frameworks that do apply can be changed or revised – sometimes quite frequently. Third, interpretations of the standards or frameworks can change. For example, after Target was breached in 2013 by a phishing e-mail to a third-party vendor, auditors became much stricter in their interpretation of the PCI standard's cybersecurity requirements. This stricter interpretation resulted in organizations that processed credit card data having to beef up their cyberdefenses across the board.

Chapter 9
Cyber Awareness

Cyber awareness involves thinking about how our daily actions affect our security posture at work, at home, and on travel. Our everyday actions and decisions can increase or decrease the chance of a successful cyberattack against our organizations, our families, or us. When we are cyber aware, we are continuously thinking about the security consequences of our actions.

Are the benefits of our online actions worth the potential cyber risks?

Cyber awareness involves thinking about what could potentially go wrong and our preparation to handle that possibility. Cyber awareness is a mindset that includes the following thoughts.

Cyber Mindset

Looking at the World Through the Eyes of Cyberattackers

Attackers are smart, capable people who are constantly trying to exploit what governments, organizations, and individuals try to protect. Attackers pursue answers to the following questions:

- *Can we get access to sensitive data such as: government intelligence, military secrets, executive correspondence, corporate proprietary information, account passwords, social security numbers, credit card numbers, bank account information, or electronic health records?*
- *Can we steal that data to sell on the open market, and what is it worth?*
- *Can we modify that data to our advantage or profit?*
- *Can we deny access to that data and profit from giving it back?*
- *Can we cause disruption or harm by changing or corrupting that data?*
- *Can we encrypt that data and profit from giving up the key?*
- *Can we use our access to sensitive IT systems to cause physical harm to devices, computers, servers, facilities, equipment, or people?*

https://doi.org/10.1515/9781501506529-009

Understanding What We Do and Do Not Do That Makes Us Vulnerable to Cyberattacks

To thwart cyberattackers, we need to be constantly aware of our daily interactions with the internet, our smartphones, and devices. We need to be aware of these interactions when we are at work, when we are at home, and when we travel. To stay cyber aware, we should pursue answers to questions such as the following:

- *How can surfing the web, opening e-mails and their attachments, and sharing data with others make us vulnerable?*
- *What can we do to make ourselves more resistant to attack?*
- *How can we protect access to our data, computers, and networks?*
- *How can we keep cyberattackers from changing our sensitive information?*
- *What preventive actions can we take to be more resistant to attack?*

Thinking If the Worst Occurs and Cyberattackers Are Successful

We will make cyber mistakes and attackers will sometimes be successful. Given the inevitability of eventually falling victim to cyberattacks, we need to plan for the worst to help minimize the impact when those cyberattacks occur. The following are representative questions to help think through potential cyberdefenses to counter attacks:

- *What can we do to detect if we are targeted by a cyberattacker?*
- *What can we do to reduce the impact of an attack?*
- *What can we do if an attacker gains access to our accounts, networks, or computers?*
- *What happens if an attacker takes control of our computer data and then denies us access to it?*
- *What can we do to resolve a cyberattack, clean up the mess, and restore our data, if a cyberattack is successful against us?*

Staying Up-to-Date on the Latest Cyberattacks, Trends, and Technologies

The cyber landscape is constantly evolving – attackers are getting smarter, but so are their targets. Keeping pace with the evolving cyber landscape and using

the latest tools and techniques takes time and energy. There are numerous resources[1] available to help answer questions such as the following:

- *How are governments, organizations, universities, colleges, and industries staying current on evolving cyber threats?*
- *What cybersecurity degrees and certificates are available from higher education institutions?*
- *What cybersecurity training courses and certifications (e.g., certified information systems security professional [CISSP]) can be obtained?*
- *What professional security conferences (e.g., DEF CON and BlackHat) provide opportunities to network with security professionals, IT professionals, and educators to stay up to date on hacking research and development?*
- *What journals provide articles on cybersecurity research, techniques, methods, and best practices?*

Adopting a Cyber Mindset

By adopting a cyber awareness mindset, we can reduce the chances of things going wrong, as well as the consequences when things do go wrong. Figure 9.1 depicts three major *cyber awareness environments* and their corresponding *things of value* that cyberattackers target.

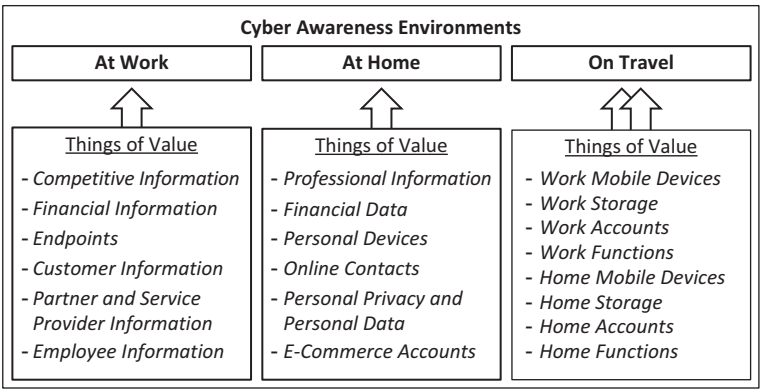


Figure 9.1: Cyber awareness should be part of our daily life, at work, at home, and on travel.

1 See Appendix D, "Online Cyber Resources," a selected compilation of references that provide insight to security awareness issues.

This chapter describes the high-level objectives of the cyberattackers, what they might want to accomplish against us, and the potential consequences. The chapter describes potential cyberattacks against our workplace and the impacts to employees, guests, contractors, and partners. Then, it summarizes cyber awareness concerns for our home and potential impacts to the workplace from our home. Finally, the chapter describes cyber awareness concerns when we travel for business or personal reasons and ways to protect ourselves from cyberattacks while away from home.

A cyber awareness mindset is thinking like cyberattackers and cyberdefenders – *at work, at home*, and *on travel*.

Things of Value: At Work

When cyberattackers attack the workplace, they can get access to and control of work computers, business accounts, account passwords, and sensitive business data. Eventually, the attackers could take control of the computing environment and hold the entire workplace hostage to their demands. Cyberattackers who compromise the workplace can cause significant damage to the organization and its employees, customers, partners, service providers, vendors, and guests.

Figure 9.2 depicts representative *things of value* that cyberattackers try to exploit in the workplace.[2] These things of value can include competitive information, financial information, endpoints, customer information, partner and service provider information, and employee information.

Cyberattackers can gain access to *competitive information* to include customer information (e.g., customer lists, contacts), intellectual property (e.g., trade secrets), strategy documents (e.g., plans, potential acquisitions), internal e-mails (some of which may be confidential), and unpublished financial data.

Cyberattackers who compromise *financial information* can steal money from online bank accounts, credit card accounts, or extort money from the organization. These attacks can be devastating to businesses, which may not enjoy the same protections against fraud as individual consumers. Ransomware attacks extort the organization by encrypting workplace computers and then holding the organization hostage until it pays a ransom to get the decryption keys. Such attacks can

2 This figure and subsequent chapter figures are adapted from Donaldson, Scott E., Williams, Chris K., and Siegel, Stanley G., *Understanding Security Issues*. Walter de Gruyter Inc., 2019.

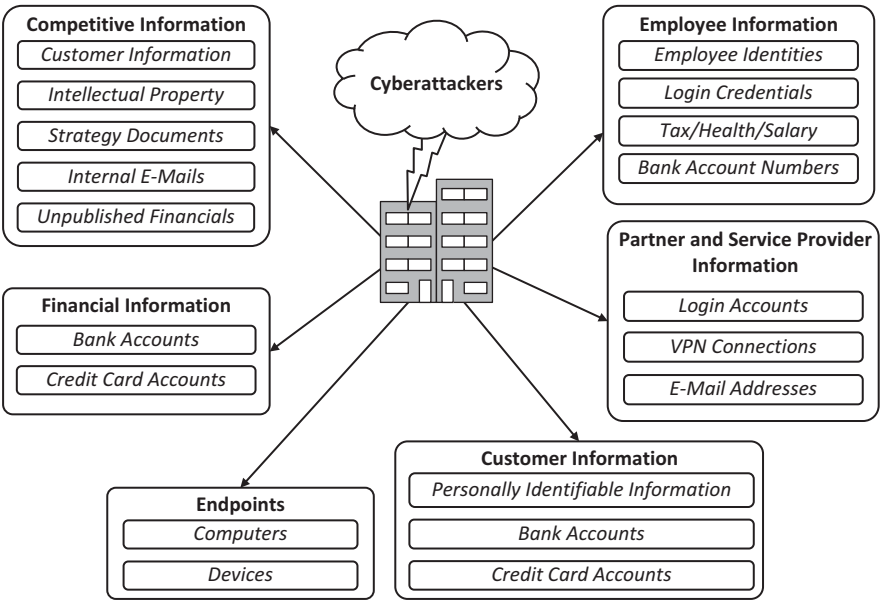


Figure 9.2: Cyberattackers have much to gain from hacking the workplace.

encrypt hundreds or thousands of computers and potentially prevent organizations from performing their day-to-day operations.

Cyberattackers use compromised *endpoints* (e.g., desktop computers, laptops, tablets, smartphones, thin clients, printers) to maintain a foothold within an organization and execute malicious code. Attackers can then use those compromised endpoints as part of a network of computers (i.e., botnet) to conduct distributed denial-of-service (DDoS) attacks, access high-value assets, or generate spam messages. Compromised endpoints can also be used to host malicious websites distributing malware or providing command-and-control functions for other cyberattacks.

Cyberattackers consider *customer information* a valuable asset because it can include personally identifiable information (PII) such as names, phones numbers, home addresses, usernames, passwords, social security numbers, passport numbers, and e-mail addresses. For those organizations performing consumer commerce with electronic transactions, cyberattackers will target their databases containing bank account numbers or credit card numbers, which can be sold to professional criminal groups for profit. Customer databases can be particularly valuable because criminals can merge and cross-reference databases from multiple breached organizations into large data sets of millions or even billions of individuals.

These cross-referenced datasets give the attackers even more information about potential victims than might be possible from a single breached database.

Cyberattackers know that an organization's *partner and service provider information* is a network of organizations that closely cooperate with each other to perform their day-to-day operations. Attackers may try to take advantage of such relationships by attacking the network connections between organizations via partner logins and virtual private network (VPN) connections. Attackers can use partner and service provider e-mail addresses or contacts to send attacks directly from one organization to its partners. Attackers know that a message from a known person at a partner or service provider organization is much more likely to be opened than an e-mail from an unknown person. Once the malicious e-mail is opened, the attackers can potentially compromise the recipients' endpoints and establish a foothold within the target organization. This foothold can then be used to launch subsequent attacks against additional people and computers.

Cyberattackers know that organizations keep significant amounts of *employee information* including their personal identities, login credentials (user identifications, passwords), tax information, healthcare information, salary data, and bank account numbers. Instead of draining the organization's bank accounts directly, attackers may choose to target employee bank accounts by rerouting employee payroll transactions to attacker bank accounts. Or, attackers may choose to sell the employees' banking information to other criminal data aggregators and fraud operators, for further exploitation.

Why can't IT security simply stop cyberattacks in the first place? Why can't computers be secure against attacks? The answers to these questions are complex, but start with the failure of endpoint security and other organization protection challenges, which trace back to the fundamental challenges of designing, operating, and maintaining complex systems. The fact is that sufficiently complicated systems are impossible to secure perfectly for an extended period of time.

A modern computer's operating system and application software are simply too large and too complex to ever be fully protected.

Endpoints will *always* be susceptible to compromise. Security will try to make endpoints less likely to be compromised via various defensive strategies. Even though security strategies may reduce the percentage of compromised endpoints, it can never ensure that the compromised percentage of devices will go to zero. Given enough time, attackers will eventually breach the organization.

Simply stated, an organization *must* assume endpoints are going to be compromised. The organization should be pleasantly surprised when endpoints are

not compromised. To protect against compromise when it occurs, an organization must layer its defenses so the endpoints most likely to be compromised first are not the most critical endpoints. When compromise occurs, the organization then has opportunities to detect and respond to the security incident before it proves disastrous. Then the organization needs to engage its recovery controls to close out the cyber incident and restore normal operations.

Things of Value: At Home

When cyberattackers attack you at your home, they can get access to your computer, accounts, passwords, e-mails, documents, pictures, and other personal information. Similar to attacks in the workplace, attackers who compromise your home can cause significant damage to your personal data, as well as your online resources like e-mail, social media, credit cards, or bank accounts. Attackers can do many things that may be harmful to you, your family and friends, or even your workplace.

Figure 9.3 depicts representative *things of value* that cyberattackers may try to exploit in the home. These things of value can include professional information,

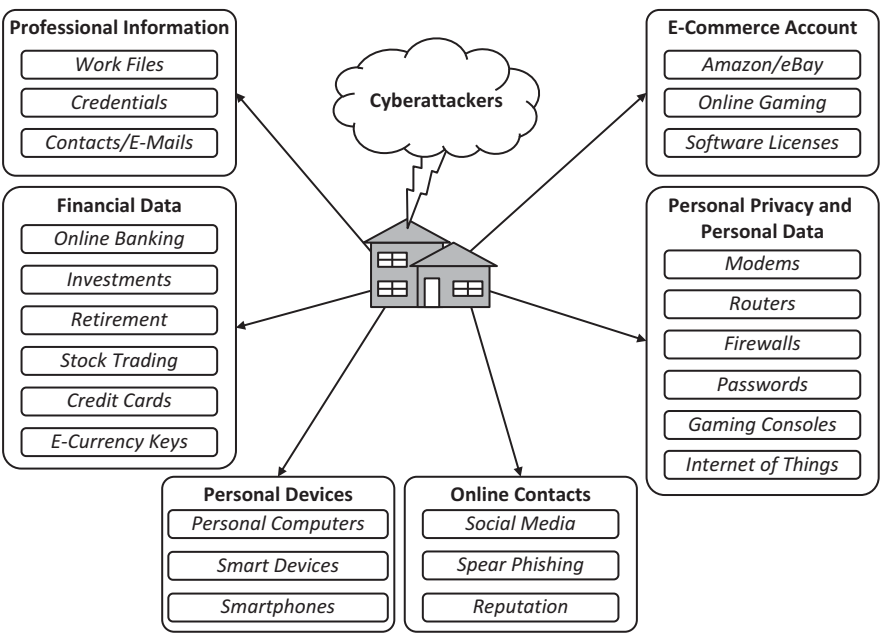


Figure 9.3: Cyberattackers have much to gain from hacking you at home.

financial data, personal devices, online contacts, personal privacy and personal data, and e-commerce accounts.

Cyberattackers can gain access to your workplace *professional information* that you may have stored on your personal devices, or that you may access from compromised personal devices. Such workplace information may include your work files, credentials, contacts, and e-mails. If attackers gain access to your workplace credentials, they may be able to impersonate you and connect to workplace systems without your knowledge.

Cyberattackers who compromise your *financial data* stored on your personal computer or device may be able to access your online banking, investments (e.g., real estate, precious metals), stock trading details, retirement accounts, credit cards, or e-currency or cryptocurrency keys (e.g., bitcoin, bitcoin cash, bitcoin gold, bytecoin, Ethereum). With this access, attackers may then be able to steal money from your online bank accounts, disrupt your investments, sell your stocks, liquidate your retirement accounts, abuse your credit cards, or liquidate your cryptocurrency. The possible good news is that you may have financial protection under the law for some of these situations, but cleaning up the mess will likely be frustrating and time consuming.

Cyberattackers who compromise your *personal devices* can use them as if they belonged to the cyberattackers. Consider the following examples of how cyberattackers can use your compromised computer:

- Attackers can conduct distributed denial-of-service (DDoS) attacks by using your computer as part of a botnet (i.e., a network of compromised computers).
- Attackers can perform illegal bitcoin mining.
- Attackers can generate hundreds or thousands of mostly unwanted e-mail messages (i.e., e-mail spam or junk e-mail) targeted to millions of internet users around the world, wasting time and resources.
- Attackers can engage in "click fraud" by manipulating your computer to "click on" *legitimate* website advertisements to generate revenue from advertisers who pay the attackers for *illegitimate* customer leads that the advertisers believe are valid.

Cyberattackers can also target your smart devices – your personal internet of things (IoT) – such as printers, home security systems, thermostats, smart refrigerators, and even some garage door openers. Such devices that are connected to the internet have unique addresses on your home network, often lack security, and may be easily infected with malware. For example, the Amazon and Netflix websites were infected with the Mirai malware by attacks launched from a botnet of such smart devices.

Cyberattackers can also hack into your smartphones (e.g., iPhones and Android-based phones). As people use their smartphones to do more of their banking and purchasing online, attackers will continue to find ways to compromise them. Smartphones should be kept up-to-date with the latest software, and users should be wary of the apps they install on smartphones from unknown providers, outside of app stores, or promising unrealistic capabilities.

Cyberattackers may obtain access to your *online contacts* and then target those contacts. For example, attackers can use your social media accounts (e.g., Facebook, YouTube, Twitter) to get information on your friends and contacts. The attackers can then "spear phish" your friends and contacts with e-mail messages crafted using your compromised information. This familiarity to your friends and contacts may increase the chance that they will succumb to the phish and install malware, reveal their credentials, or divulge other information. Using your online contacts, attackers can potentially damage your reputation by making derogatory public posts in your name or by causing harm to people who trust you.

Cyberattackers may attempt to invade your *personal privacy* or destroy *personal data* by extorting you directly for money, services, or property through threats, violence, or other illegal methods. Attackers may try to attack your home network devices, such as modems, routers, firewalls, gaming consoles, and other IoT devices. Once your home network is compromised, the attackers may use various methods to invade your personal privacy or destroy your personal data. They may also try to extort you for money using ransomware, fake antivirus alerts, Internal Revenue Service (IRS) and Federal Bureau of Investigation (FBI) fraud, image blackmail, or holding your data hostage. Similar to workplace environments, attackers can use ransomware (e.g., Cryptolocker, WannaCry, Petya) to encrypt your personal computer's files and then hold them "hostage" until you pay the attacker to decrypt the files. Extortion payments may be via cryptocurrency (such as bitcoin) or credit card. Of course, even if you pay the attacker, there is no guarantee the attacker will decrypt your files. The FBI recommends not paying ransoms, as payment rewards the criminal and contributes to more ransomware attacks in the future. Among other proactive cyberdefense activities, you can counter ransomware attacks by frequently backing up your computer files.

Other cyberattacker extortion activities include the use of fake antivirus alerts (e.g., website ads, website popups) to scam you into revealing your credentials or paying for IT repairs you don't really need. For example, a fake antivirus alert may tell you your computer is infected and provide you a phone number to call to resolve the issue. If you call the phone number, the attacker's "customer support" personnel may try to charge you hundreds of dollars to fix the problem. Attackers may also impersonate the IRS or FBI to trick you into

thinking you have run afoul of the government. For example, attackers inform you that you are required to pay penalties to "clear up" your alleged crime. Cyberattackers can use intimate images on your computer or compromising images taken from your webcam camera to blackmail you. For example, attackers may threaten to post the webcam images on social media unless you pay them a ransom. Another extortion situation may involve your personal correspondence or photos. Cyberattackers may steal your correspondence or digital photos, hold them hostage, and demand payment before they are returned to you.

Cyberattackers may target your *e-commerce* accounts, such as Amazon and eBay, and corresponding transactions. Attackers can access and use your accounts and transactions to create fraudulent transactions in your name to benefit themselves. For example, attackers may access your Amazon account and set up a new Amazon Prime account[3] for themselves. Attackers may even access your online gaming systems (e.g., Fortnite or Roblox), steal your "in-game" credits or currencies (similar to digital currencies), and then convert them to real-world money either by converting them directly or by selling them to other gamers. Finally, your computer's software may have "license" keys or "upgrade" keys that the attackers can steal and then sell on the black market for profit.

There are robust markets for your *things of value* on the "dark web" criminal internet. The dark web is comprised collections of websites on encrypted networks that require specialized software and authorization to access. Cyberattackers will attempt to exploit you at home, access the dark web, and then sell what they can to others who may then attempt to exploit you again!

Protecting Yourself On Travel

When cyberattackers attack you on travel, they may be able to get access to the devices and information you are carrying with you, and then exploit that access to attack your workplace and home computing environments. When you travel, you may carry both *workplace* and *home* computing devices with you (e.g., laptop computers, smartphones, tablets, or specialized eReaders such as Amazon Kindle), as well as removable storage devices (e.g., universal serial bus [USB] thumb drives, external hard drives). Figure 9.4 depicts representative *things of value* that cyberattackers may try to exploit while you are on travel. These things

3 Amazon Prime is a subscription service that provides paid subscribers access to services that would normally cost a non-subscriber additional money (e.g., faster delivery times, streaming music).

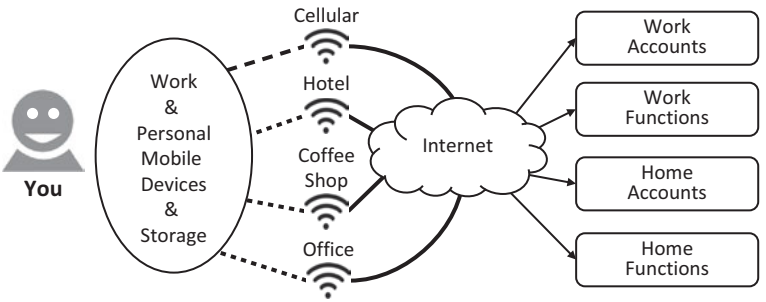


Figure 9.4: On travel, you are especially vulnerable because you are using mobile information technology that is fundamentally less protected than at work or at home.

of value can include your physical devices, along with work accounts, work functions, home accounts, and home functions.

When you are on travel, you may also be connecting to the internet using available Wi-Fi or cellular networks that are managed by providers different from your normal providers, and perhaps with different protections as well. You may stay at hotels with non-secure internet connections or use non-secure connections at a local coffee shop. Connecting to such internet connections provide cyberattackers with opportunity to attack you directly, or through other people who are simultaneously connected to the same non-secure connections.

What are the cybersecurity risks related to traveling with information technology? How can you reduce those risks through preparation and planning? This section addresses these questions by describing the following related cyber aware travel topics and tips.

What to Take

When traveling, only take what you need for what you plan to do during the trip. This can be particularly true for international travel, where taking certain sensitive data outside of the country can cause you to run afoul of export control regulations and national intelligence agencies.

- Consider purchasing separate media (e.g., laptops, removable storage) for travel, rather than taking devices containing thousands of files you definitely will not need. Alternatively, consider removing unnecessary files and data from the devices you are taking, if having separate devices is infeasible.
- Consider putting the files you do need on an encrypted thumb drive or other protected media. Hardware-protected devices are even better.

- Keep additional files you might need in the cloud, as well as backup copies of the files you take with you.
- If you are accessing only one or two of your work accounts, do not take a password file that contains passwords to your other accounts.
- Check with your organization before taking organization equipment on travel, especially if the travel is international. Work with your organization IT or industrial security office to remove sensitive information not needed for the trip from your devices.
- Consider buying a prepaid mobile phone when traveling internationally to reduce risk of using your primary or personal phone in another country.
- Put screen locks on your computers and mobile devices, and use hotel safes to lock up equipment when it is not in use. Remember that hotel staff *can* get into hotel safes, so it is a deterrent but hardly fail-safe protection.

Smartphone or Tablet Protection

Modern smartphones and tablets pack tremendous computing power, storage, and connectivity into a relatively small footprint. If you phone is lost or stolen, especially while on travel, personal data contained on it becomes vulnerable to theft or abuse. Smartphones with the latest cellular technology have more powerful high-speed transmission rates, multimedia access, global roaming, and secure connections than earlier technology generations. With good signal quality, such smartphones can act as an internet service provider (ISP) hotspot that you can use instead of public Wi-Fi for your laptop computer. Cellular data connections tend to generally be more secure and private than public Wi-Fi. Make sure to configure your personal hotspot with a strong password.

- Consider putting a screen lock on your device using a password, a personal identification number (PIN), biometric authentication, or facial recognition. Back up your device, or configure it to backup automatically to a cloud service.
- Activate phone features that allow you to locate your phone if it is lost or stolen, as well as the ability to remotely delete the data on your phone when it connects to the cellular network.
- Consider signing up for insurance to cover device replacement if it is lost, damaged or stolen.
- Carry a backup device – perhaps last year's old phone – that you can quickly activate through your carrier or by swapping out the subscriber identity module (SIM) card from your primary phone.

Bluetooth and Wi-Fi Networking

Mobile devices have a variety of wireless technologies built in, including cellular, Bluetooth, and Wi-Fi networking. Noncellular tablets still tend to include Bluetooth and Wi-Fi for local networking. When these wireless networking technologies are enabled, others can see and potentially connect to your devices. Cyberattackers can use these connections to attack and possibly exploit your devices, if they are vulnerable.

- Disable Bluetooth or Wi-Fi networking when you are not using them.
- Be cautious when connecting to public Wi-Fi networks (e.g., at coffee shops, hotels, or convention centers) and disable "automatic Wi-Fi connection." Only connect to public Wi-Fi when necessary and make sure your subsequent connections and web browsing use encrypted protocols.
- Make sure wireless hotspot features are disabled when not in use and password-protected when you are using them.
- When using wireless hotspot features of your phone or mobile devices, make sure they are protected with a strong password.

Kiosk Computers

Using "kiosk" computers or public Wi-Fi network connections increases your risk and must be considered accordingly. Kiosk computers are notoriously unsecure and should be assumed to be compromised, so reduce your use accordingly.

- Consider using a thumb drive for files and travel papers, rather than accessing sensitive e-mail or online cloud accounts from a kiosk computer.
- Use a thumb drive with a hardware write protection feature so that a kiosk computer cannot attempt to infect the thumb drive with malware.
- If you have to enter sensitive credentials on a kiosk computer, try to change them soon afterward from a trusted device.

Public Internet Connections

Public networks can be very dangerous. Other computers on the same network may be able to scan your computer for vulnerabilities and attempt to compromise it. The network may be able to monitor everywhere you go and everything you do. This monitoring may include intercepting your connections to trusted websites and capturing your usernames and password credentials. Sometimes,

cyberattackers will stand up malicious networks that use common names like "public Wi-Fi," "hotspot," "coffee shop," "lobby," or "guest," to trick unsuspecting users into connecting.

- Ensure the built-in firewall is enabled on your devices, along with other defenses like network filtering and anti-malware software.
- Be cyber aware and watch for signs of a cyberattack, such as unsolicited messages, unexpected invitations, pop-ups, or attempts to install software.
- Try to only use wireless networks that are password-protected instead of unprotected "open" networks.
- If you have access to a virtual private network (VPN) connection, immediately connect to the VPN so your outbound traffic is private and encrypted.

Hard Drive and Mobile Media Encryption

On your mobile devices and computers to be used on travel, enable storage encryption for built-in and removable storage, so that loss of a device or drive will not result in the compromise of its data.

- For Android-based phones, the "Security Settings" area includes an option for encrypting the phone and micro Secure Digital (microSD) removable storage.
- For Apple phones, encryption is enabled by default once a passcode is put in place.
- For your laptop, enable drive encryption to prevent someone from removing the drive and simply copying its data. The encrypted drive will not be accessible until the user enters the drive encryption password while the computer is starting up. Windows includes "BitLocker" drive encryption built-in, while Apple's operating system has "FileVault." Linux distributions usually include the "dm-crypt" and "LUKS" open source encryption tools.
- Removable hard drives and solid-state drives can usually be encrypted using the same tools as the primary drives on laptop or desktop computers.
- If the removable media is to be used with multiple computers or operating systems, make sure all computers have the appropriate encryption software installed, or bring the software with you. Alternatively, you can use third-party tools such as McAfee or Symantec disk encryption tools that include support for multiple computer platforms.

Note that encryption can make data recovery from a failed drive difficult or even impossible. Minor failures of encrypted drives can make your computer unable to boot or access your files, even when most of the data is otherwise

intact. So, backups are essential when encryption is used. Make sure you have backups of your encrypted operating system, applications, and data.

Backups and Contingencies for Travel

Make multiple backups of your most critical information and identity documents. Keep those backups and copies in separate locations, so a single lost bag or stolen wallet will not be disastrous.

- Think through where you can go for help. Have phone numbers for local consular offices, tourist assistance offices, and your hotel. Make sure someone back home has this information in case you need their help. If you are traveling on business, get the contact information for your organization's security and travel offices.
- Back up your electronic files and do not take anything with you that cannot be replaced from a backup located on removable media or in the cloud.
- Consider taking two complete wallets where each has an ID, separate credit card, cash, and other important documents.
- If your passport is lost or stolen, even an expired driver's license can be helpful for proving who you are to government officials. Photocopies or pictures of your passport, birth certificate, driver's license, and other personal identity documents are even better.
- Consider taking digital photographs of your passport, itinerary, and tickets, and keeping them on your smartphone, protected by a password.

Physical Protection, Personal Safety, and Electricity

When traveling internationally, check with your government (in the United States, www.state.gov) for guidance and warning specific to the country and region where you are going. If traveling on business, also check with your organization's security office for guidance.

- Find out your nation's embassy and consular office addresses and telephone numbers in the country and city you will be visiting.
- When staying in hotels, lock your valuables in the hotel or room safe. If no safe is available, place valuables in drawers or suitcases where they are out of sight and not obviously present. When not locked in a safe place, carry your valuables with you.

- Avoid keeping wallets in bags or back pockets where they may be visible and pickpocketed or easily taken.
- For personal or business computers, use carry cases that do not look like they contain computers.
- For the places you stay, walk the fire escape routes (primary and secondary) and make sure the routes actually lead outside of the building. Watch out for locked doors, building repairs, or construction that may block escape routes.
- To increase the endurance of your smartphone or mobile devices, bring rechargeable universal serial bus (USB) batteries. Also bring at least one spare charger and charging cable, in case your primary one breaks or is lost.
- Bring multi-voltage digital power adapters that accept power from most places in the world. Since electric wall plugs are not standard, find out what the plug types are for each area you visit and bring appropriate adapters. Note that some countries may use multiple types of power and multiple types of plugs, depending on the specific region or city you are visiting.

Conversations and Online Sensitive Data

Be cautious about what you say, what you type, and what is visible on your device screens, as you do not know who is standing next to you or looking over your shoulder at the airport, on the plane, or in the lobby of your hotel. When traveling on business in foreign countries, remember that government officials may be working closely with your customers or your competitors to capture business intelligence from you and your colleagues.

- Do not discuss your organization's business, personal matters, or various account numbers (e.g., credit cards) in the hotel lobby or other public area.
- Install a screen lock on your laptop and mobile devices and configure it to automatically lock after a period of inactivity (e.g., 15 minutes).
- Install privacy screens on your devices to make it harder for people looking from the side to see your logins, credentials, account numbers, contacts, or phone numbers.
- Be aware of people sitting or standing behind you or too close to you. *Can they see your laptop screen? Could they watch you type in your credentials?* Do they seem to be paying attention to you, or what you are doing? Orient yourself so people around you cannot see what you are doing.

Diplomacy, International Traffic in Arms Regulations (ITAR), Export Administration Regulations (EAR), and Security Clearances

When traveling internationally, you become part of international diplomacy whether you want to be or not. Understand that your actions reflect your country, and that even minor transgressions can quickly turn into long, drawn-out international incidents.

- Be aware of international laws and politics, as each country has different rules regarding data handling, merchandise for demonstration (think samples), prescription drugs, and controlled substances.
- Make sure you have all the appropriate paperwork and doctor's orders for prescription drugs, particularly narcotics. Understand what is and is not allowed for each country you are visiting.
- If your organization handles export-controlled data or highly proprietary commercial data, know what data is on your devices and media and consult with your organization to make sure you follow proper procedures for protecting against an international breach of sensitive data.
- If you have a security clearance, check with your organization's security office to understand your responsibilities, including pre-trip and post-trip reporting requirements.
- Plan for things to go wrong (e.g., lost luggage, lost phone, stolen laptop) and have contingency plans.
- Make sure people know you are traveling and who to contact in case something happens to you.

As the cyber world continues to grow exponentially, its complexity and vulnerability will also increase, as will potential cyberattacks to exploit it. Laws and regulations will continue to struggle to keep pace with the cyber world, our digital lives within it, and the protections it requires. To protect ourselves and our organizations, cyber awareness is an increasingly important part of our daily lives and culture.

Chapter 10
Organization Cyber Awareness

Organization cyber awareness involves thinking about how the interwoven activities of personnel, customers, partners, service providers, vendors, and guests can affect an organization's security posture. Technology and service capabilities supporting these activities are evolving at "e-commerce business speed," but cyber threats are also evolving as quickly, or even faster.

Crackers and other cybercriminals release 400,000 new malware variants every day and send 29 billion spam emails. The number just keep going up and up.[1]

Staying up to date on the latest cyberattacks, trends, and technologies is a daunting task. Similarly, staying current on the latest IT infrastructure tools, technologies, and processes needed to deliver the required, sophisticated capabilities to authorized users and protect the organization is a nonstop task. Consequently, typical organization IT environments are becoming increasingly complex, as depicted in Figure 10.1.[2]

Organization computer networks often include: (1) internet connectivity, (2) Wi-Fi connectivity, (3) work functions, and (4) internal and external network infrastructures. Authorized users use such networks to work with data that may be sensitive, regulated, or government classified. Such data may require specialized handling procedures or additional cyberdefenses to ensure that the data is properly protected.

This chapter starts by contrasting a couple of significant differences between cybersecurity protection at home and at work. The chapter then describes organizational cyber awareness in terms of some of the major topics that should be considered by the people using the organization's IT systems. These topics are different from cybersecurity capabilities, since not all capabilities are typically visible to all users. These topics have been selected because they are topics of awareness at many organizations using IT technologies. Since there is no single way to implement organization cyberdefenses, you should understand your organization's actual IT environment and cyberdefenses, and consider your users' specific responsibilities to support the organization's cyber protections.

---

1 Sjouwerman, J. *Cyberheist: The biggest financial threat facing American businesses since the meltdown of 2008*. KnowBe4, Clearwater, Florida, April 20, 2016.

2 Figure is adapted from Donaldson, Scott E., Williams, Chris K., and Siegel, Stanley G., *Understanding Security Issues*. Walter de Gruyter Inc., 2019.

https://doi.org/10.1515/9781501506529-010

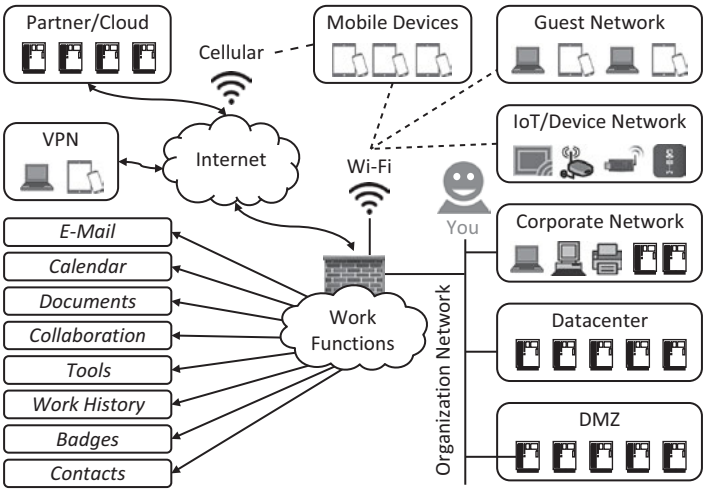


Figure 10.1: Organization computer networks are increasingly interconnected and complex.

Organizational Cyberattack Sequence

There is a significant difference between personal cybersecurity protection for a computer network at home versus the protection needed for a computer network at work. At work, professional cybercriminals, hacktivists, and nation-state attackers may use *advanced attack techniques* to target organizations containing concentrated, valuable information. Attackers can make considerable investments to compromise more heavily defended organization networks versus more lightly defended home networks. Due to the complexity of organization networks, and the need for attackers to take steps to reach their targets within those networks, organization cyberattacks can be analyzed in terms of a *cyberattack sequence* that progresses from the initial incursion to the attackers achieving their objectives.

Figure 10.2 illustrates one version of this cyberattack sequence that contains five major steps.[3] Once the attackers establish a foothold within the organization, they may go through multiple cycles of the cyberattack sequence steps 2, 3, and 4, navigating the target organization's IT environment until they reach their objective. Attackers may cycle through command-and-control activities, escalation

3 Figure adapted from Donaldson, Scott E., Siegel, Stanley G., Williams. Chris K., and Aslam, Abdul, *Enterprise Cybersecurity*. New York: Apress, 2015.

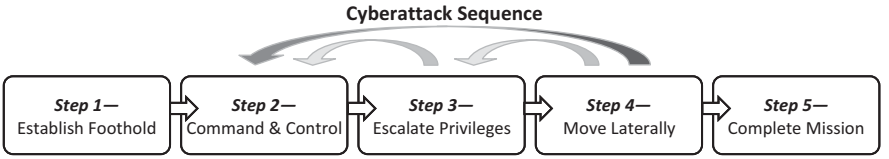


Figure 10.2: Advanced cyberattackers will often follow a cyberattack sequence to compromise their targets and complete their missions.

of privileges, and lateral movement multiple times between their initial foothold and the completion of their mission. It is important to note that these cyberattack sequence steps may not always be executed exactly in sequence. Sometimes attackers may escalate privileges before they establish command-and-control, or they may move laterally before escalating privileges.

Organizations should be aware of the advanced cyberattack sequence and consider it in their cyberdefenses. Cyberdefenses do not only prevent attackers from establishing their foothold. Instead, cyberattacks can defend all along the attack sequence. E-mail, web, and endpoint defenses can make it harder for attackers to establish a foothold within the organization, and may be able to detect when a foothold has been established. Network perimeters may be able to detect when attackers attempt to establish command and control, and can block command-and-control traffic that uses known malicious traffic patterns. Identity and access management systems can make it harder for attackers to escalate privileges, and may be able to detect when privilege abuse is occurring. Internal sensors may be able to detect attackers moving laterally, while network segmentation may be able to block lateral movement from occurring. Finally, hardened infrastructure and data protection controls may be able to stop attackers from accomplishing their mission, even after all other protections have been defeated. All of these protections, working together, constitute the organization's full cyberdefense against advanced cyberattacks.

Against advanced cyberattacks, an organization needs the ability to dynamically respond to cyberattacks by isolating, containing, and remediating them so the attacker's efforts are disrupted, giving defenders time to maneuver in response. Such cyber defense in depth and resilience against attack are not typically found in home computing environment. Against organizations, professional attackers can take control of the victim's IT environment and use it to cause damage that can impact thousands of employees, customers, partners, service providers, or vendors.

Another significant difference between cybersecurity protection at home and at work involves the laws and regulations that apply. The payment card

industry data security standard (PCI DSS) requires merchants (and processors) to implement cybersecurity protection for stored credit card data. The European Union (EU) General Data Protection Regulation (GDPR) provides extensive online privacy protection for EU citizens regarding their personal data, and specifies significant fines for non-compliance or breaches. The U.S. Sarbanes-Oxley Act (SOX) law requires strict financial accounting and cybersecurity controls for public companies to protect investors against fraud. The Health Insurance Portability and Accountability Act (HIPAA) specifies strict controls around the use and disclosure of an individual's health information. Similar laws to these have been passed in many countries around the world, including Germany, France, and Japan.

Because of these differences, it behooves organizations to make sure their personnel are aware of the organization's cyber policies and cyberdefenses, and are ready to play their part in supporting those cyberdefenses. Figure 10.3 shows some of cyber awareness topics that authorized users should know as they help the organization defend against the full range of amateur and professional cyberattackers.

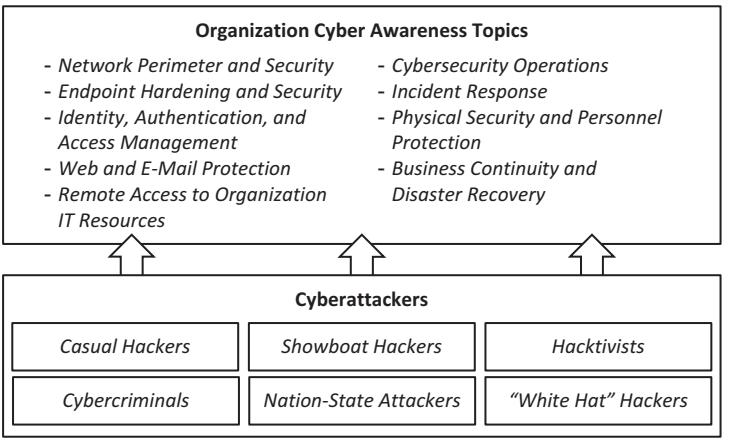


Figure 10.3: Organizations must make their personnel aware of many topics in cybersecurity to help the organization defend against a wide range of potential cyberattackers.

Network Perimeter and Security Cyber Awareness

This cyber awareness topic involves the security of organization networks, their services, and access to them from the internet and internally connected devices. These capabilities provide for filtering and monitoring of network traffic to

block potential malicious network traffic and detect attacker network traffic when attacks occur. For example, network "preventive" controls can block potentially malicious network traffic based upon its source, destination, port, protocol, signature, or other properties. This blocking can make it difficult for attackers to connect to organization resources and control them remotely.

Organization personnel should be aware that when they are connected to the organization's network, they are behind the organization's network perimeter and protected by its network security preventive and detective controls. Some specific aspects of the organization's network perimeter and security to consider are as follows.

Firewalls

These security systems filter out unwanted network traffic by monitoring and controlling ingress and egress network traffic between an organization's computer systems and the internet. Firewalls establish a boundary around the organization's network and are designed to block unauthenticated connections from outside the network. Firewalls may include: packet-filtering, circuit-level gateways, stateful inspection, and application-level gateways (also known as proxy firewalls).

There are also next-generation firewalls that include inspection technologies alongside of network filters. For example, deep packet inspection technology can be combined with intrusion detection systems and intrusion prevention systems (IDS/IPS) to inspect and block malicious network traffic at a more granular level than traditional firewall inspection technologies. Cyber defenders can use these technologies to recognize certain cyberattacker activities and command-and-control patterns, enabling detection and response against network-based cyberattacks.

Organization personnel should be aware that firewalls protect them when they are connected to internal organization networks, and can block or detect a multitude of potential cyberattacks. When users take organization computers outside of the network – like with laptop computers connected to home or public networks – these protections may not be available, resulting in dramatically increased vulnerability to certain types of cyberattacks.

Guest Networks

These networks are designed to enable visitors to use their own devices (such as laptops or tablets) to connect to the internet, while isolating the visitors and

their devices from an organization's network of computers, servers, and data. This guest isolation approach helps keep the organization secure because visitor devices are prevented from being used to attack the organization from inside its network.

Guest networks may be wired or wireless and may or may not be password protected, requiring visitors to get the password of the day. Visitor network access passwords should be changed regularly to reduce the risk of visitors being able to connect long after their visit was concluded. Guest networks may also limit visitors in terms of bandwidth priority, network speed, and access to internal organization resources such as applications or printers. Organizations should monitor guest networks to ensure that only authorized visitors are connected and are using the networks appropriately.

Organization personnel should be aware that guest networks should be isolated from the rest of the organization's IT environment, and that activity on guest network may be monitored to detect potentially malicious activity. There may be no privacy on organization networks! Visitors who connect to guest networks may have to go through multiple steps to connect to the guest networks, and may find that even then, their activity is still restricted.

Secure Wi-Fi Networks

These wireless networks provide organization personnel with a secure way to connect to organization networks from mobile devices and laptop computers. Secure Wi-Fi networks are widely used in many industries and should be configured for greater security than similar wireless home networks. For example, manufacturing plants and hospitals may use secure Wi-Fi for numerous mobile devices that need connectivity while moving around the plant facility or hospital. Secure organizational Wi-Fi networks typically have passwords that change frequently, or require multifactor authentication (MFA) tokens or certificates to authenticate connections.

Organization personnel should be aware that Wi-Fi networks, like guest networks, are likely going to be secured and monitored. Personnel should be aware that facility Wi-Fi networks will likely be detectable outside of the building, and that attackers may attempt to connect to those networks from far outside the organization's buildings and physical security. Personnel should not stand up their own Wi-Fi networks or "hotspots" within organization facilities without prior written approval and appropriate protections in place.

Endpoint Hardening and Encryption Cyber Awareness

This cyber awareness topic involves the protection of endpoint computing devices such as personal computers, servers, and mobile devices that access organization data. Organization-issued personal computers may be configured to limit employees from customizing their systems, reducing the risk of introducing malware and other cyber threats. Organizations may also install computer endpoint security suites such as anti-virus, anti-malware, host firewall, intrusion detection, or encryption. Additional endpoint hardening may include configuring systems with security policies for access control, privilege management, or tools for auditing and forensics. Standardization of endpoint configurations helps the organization's IT personnel manage large numbers of desktop, laptop, and server computers.

Mobile devices use operating systems that are different from personal computer operating systems, requiring different toolsets to provide basic functionality. Mobile devices are frequently personally owned, which means organizations may have to treat them like the user is accessing organization systems from noncorporate home computers. Regardless of whether the endpoint is owned by the organization or the individual, the goal of endpoint security is to (1) prevent attackers from taking administrative control of endpoints that store organization data, (2) detect attempts to take administrative control or maliciously access organization data, and (3) facilitate the investigation of incidents when compromises of systems or data are suspected.

Endpoint security can *never* be assumed to be 100% effective, as administrators make mistakes, viruses proliferate, and exploits for vulnerabilities are easily obtained by well-resourced attackers.

Organization personnel should be aware that when they use the organization's endpoints, they are protected by the organization's endpoint hardening and encryption preventive and detective controls. Some specific aspects of the organization's endpoint hardening and encryption to consider are as follows.

Central Endpoint Management Tools

These software tools can provide inventory management and asset control of organization equipment, as well as monitoring what software is installed and running on endpoints. Central endpoint management enables organizations to comply with software license agreements, accounts for cybersecurity business drivers (such as legal or regulatory requirements), and enforces internal policies

and standards. Central endpoint management also helps with managing, installing, and verifying software patches, which helps the organization stay protected against evolving threats.

Organization personnel should be aware that organization-owned endpoints may be centrally managed, with administrative access, software installation, and configurations tightly controlled. Endpoint users may be prohibited from installing their own software, or may have to go through procedures to request or authorize software prior to installation. In addition, many types of endpoint configuration changes may require requesting permission, or putting in a service ticket with an endpoint management help desk.

Endpoint Hardening and Monitoring

These security approaches involve "locking down" or "hardening" endpoint computers and devices. Hardening can include configuring systems with special security policies, anti-malware software, and other tools to reduce vulnerabilities and make the systems less susceptible to cyberattacks. It may also involve removing operating system tools that are superfluous, or vulnerable to attack. Hardening may also include installing software that monitors endpoint device activities for unauthorized applications or user activity. Such software can send alerts on suspicious endpoint behavior to central administration consoles for tracking and analysis.

Organization personnel should be aware that organization-owned endpoints may be configured with "hardened" security configurations, as well as extensive monitoring to detect security events or incidents. System hardening may include the removal of local administrator privileges, disabling of features like internet access or document printing, or configurations that require connection to organization networks full-time. In extreme cases (such as for securities traders), endpoints may record all user activities and keystrokes for later audit and review.

Full Disk and Media Encryption

These technologies protect data stored on endpoints and mobile devices, including thumb drives and external hard drives. Full disk encryption protects data by converting it into unreadable code that is difficult to decrypt and can prevent unauthorized access. Authorized users must provide the encryption

key – such as a password, passphrase, one-time password, or biometric such as a fingerprint – to access the encrypted data. Encryption can be optional at home, but in the workplace, it may be required by regulation. When organization endpoints and removable media are encrypted, lost or stolen devices may not have to be reported to regulators or the public.

Organization personnel should be aware that organization-owned endpoints may be configured with full disk and media encryption. The organization may also have media encryption enabled to protect removable media like external hard drives or universal serial bus (USB) thumb drives. This feature protects organization data on those devices, and can allow the organization to avoid serious regulatory impacts if devices are lost or stolen. In addition, removable media encryption may make sharing documents outside the organization extremely challenging.

Data Classification and Data Loss Protection (DLP)

These security capabilities keep track of what types of data are stored on organization endpoint systems, and potentially shared outside the organization. Such capabilities may be able to monitor, detect, or block potential data breaches and data exfiltration transmissions. For example, if an authorized employee accidently attempts to e-mail a list of employee social security numbers outside the organization, DLP software may detect the message and alert central administration consoles. The software may also be able to block the transmission and force the user to request permission before transmitting the sensitive information outside the organization.

Organization personnel should be aware that organization-owned endpoints may be subject to the organization's data classification and DLP efforts. Personnel should be aware of the organization's data classification and protection policies, as well as its regulatory obligations regarding the identification and protection of sensitive data. When users create documents, they may need to classify those documents in terms of their scope and sensitivity. Usually, this classification is done using application plugins and dropdown menus. When DLP is in use, personnel should understand that every document they create, message that they send, or website they visit will be scanned to detect attempts to send sensitive data outside of the organization.

Identity Management, Authentication, and Access Management Cyber Awareness

This cyber awareness topic involves enabling authorized individuals to securely access organization resources, and managing the permissions they have when they access those resources. Identity management ensures that accounts and accesses are provisioned, de-provisioned, and periodically re-certified according to the organization's policies. Authentication ensures that people who are accessing organization systems are who they say they are. Access management ensures that users do not have privileges to systems that exceed their roles in the organization.

Organizations expect people who have access to their networks to be cleared and authorized.

Organization personnel should be aware that when they are using organization accounts and online identities, they are being protected by the organization's identity management, authentication, and access management preventive and detective controls. Some specific aspects of the organization's identity management, authentication, and access management to consider are as follows.

Identity Life Cycle Management

Identity life cycle management is a series of interrelated steps that involve the administration of an authorized user's identity, and can include user accounts, digital certificates, roles and permissions, access profiles, and group memberships.[4] In general, organizations provision accounts needed for personnel, customers, partners, service providers, and vendors. Accounts and accesses are granted when they are needed, so this process seldom presents a problem. Organizations should also de-provision such accounts when turnover occurs (when an employee leaves the organization), or when roles change. De-provisioning of accounts and accesses when they are no longer needed can be problematic, since the departed user is not asking to be removed. To address this problem, organizations should also re-certify accounts and permissions so that unused accounts and permissions can be removed. This activity should be carefully designed to include all

4 Identity life cycle can also be shared between physical access control systems and electronic, or logical, access control systems. Advanced life cycles may include issuing and managing smart card badges that are used for both physical access to facilities and logical access to computer systems.

accounts, permissions, applications, and systems. The more decentralized the organization, the harder the re-certification process can be to complete successfully.

Organization personnel should be aware that their organization electronic identities need to be provisioned, maintained, updated, and retired over the course of their life cycles. Keeping identities and permissions up to date is a constant challenge, but very important to the organization's overall cybersecurity posture and regulatory compliance. Personnel involved in identity and permission re-certifications should take their responsibilities seriously and diligently check that all identities and permissions are really in use and necessary.

Third-Party Account Management

This process includes managing accounts belonging to partners, contractors, and other third-parties with access to the organization's IT systems. These accounts can pose a unique threat to the organization because they belong to people outside the organization who may not be subject to its identity life cycle processes, and who may not inform the organization when their role or employment changes. Frequently, third-party personnel have access to the organization's IT systems using remote access tools, which can pose an additional risk. It is not uncommon for cyberattackers to get access to a large, well-defended organization by targeting its suppliers or partners, and then use their access to get into the target organization's network.

Organization personnel should be aware that third-party accounts are a possible gateway into the organization from outside partners and contractors. Third-party organizations and their people may not be diligent in asking that accounts or accesses be removed when no longer needed. This leftover access can leave open back doors into the organization's IT environment. Organization personnel need to be diligent in monitoring third-party accounts and accesses, and removing them when they are no longer needed.

Single Sign-On (SSO)

This access control capability enables employees to log into different organization services using a single set of account credentials, usually a single organizational user ID and password or multifactor authentication (MFA) token. This capability can be a significant improvement in usability compared to requiring separate credentials for each service. Frequently, SSO is implemented by requiring users to logon once – usually through a central website – to access multiple

organization services like e-mail, calendar, sales, finance, and human resources. Of course, if an attacker can compromise that single set of SSO credentials, then they will gain access to all of those organization services, as well.

Organization personnel should be aware of how SSO capabilities work, and how those capabilities make their lives easier. They should also be aware of how SSO can dramatically increase the damage that can occur when even a single account gets compromised. Personnel need to be tolerant when some organization services are not SSO-enabled. SSO integration is complex and expensive, and enabling SSO for all organization applications may not be cost-effective.

Multifactor Authentication (MFA)

This security mechanism involves requiring more than one type of authentication factor to verify users' identities prior to accessing organization IT resources. MFA may also be referred to as two-factor authentication (2FA) or strong authentication. Authentication factors can include something you know (password, personal identification number, passphrase), something you have (a token, smart card, or mobile device), or something that identifies who you are (a biometric such as a fingerprint or facial geometry). Requiring multiple factors for authentication makes it significantly more problematic for attackers to impersonate users over the internet.

Organization personnel should be aware that MFA capabilities are one of the organization's strongest protections against credential abuse, particularly over the open internet. Personnel should keep track of their physical or virtual tokens, and take care to not install virtual token software on devices that are insecure or poorly protected. Professional attackers may become aware of an organizations' MFA requirements, and may try to trick personnel into giving up their MFA credentials in a cyberattack.

One-Time Password (OTP) and Out-of-Band (OOB) Authentication

These security mechanisms are a commonly used method for delivering MFA capabilities to large organizations. OTP is a one-time use password that is generated by a token or virtual token device, and then used for logging into an organization's network or websites. OOB authentication involves requiring the user to verify their identity using a trusted communication channel that is separate from the primary communications link. OOB may be delivered using a

mobile device or over the phone, and reduces the risk of a "man-in-the-middle" attack being able to intercept user credentials.

Organization personnel should be aware that OTP and OOB authentication are powerful forms of MFA, and are commonly required for remote access to organization resources. While adding extra steps for connection approvals and authentication codes can be cumbersome, these MFA techniques add considerable security beyond what is provided by traditional username and password authentication.

Privileged Access Management

This security mechanism involves deploying a "vault" in the organization's IT environment that generates secure credentials for sensitive organizational accounts, and then manages the access to those accounts. This capability is usually used for systems administration accounts, service accounts, and other highly privileged accounts that can deploy or reconfigure organization IT systems, applications or data. Privileged access management systems may require MFA before these accounts can be checked out, may record the sessions using these accounts, and may change the passwords of these accounts automatically, on a regular basis. For the most sensitive accounts, privileged access management systems may even change the passwords of the accounts every time the accounts are used, to defend against password replay attacks or abuse of cached credentials.

Organization personnel should be aware that privileged access management capabilities may be the organization's last line of defense against advanced cyberattackers who have penetrated the outer cybersecurity perimeter. Consequently, administrators with access to privileged access management accounts should treat their access very seriously, protect their access, take as few chances as possible, and report any anomalies or signs of compromise.

Web and E-Mail Protection Cyber Awareness

This cyber awareness topic involves protections tailored to specific applications such as web browsing and e-mail. Web protections may be applied to users' web browsing and filter the websites they may visit, along with the content that may be downloaded from those sites. Web filtering may determine whether web page content should be displayed to a user by checking its origin or content against known malicious websites. Similarly, e-mail protection may filter incoming e-mails for malicious attachments and links to malicious websites containing computer viruses, worms, ransomware, spyware, or other objectionable content.

These protections reduce the likelihood of organization computers or devices being compromised by malicious websites, e-mail messages, or document attachments. These protections may only be available when employees are in the office and connected to the organization network, or the protections may be provided all the time through endpoint protections or "always-on" virtual private network (VPN) connections.

Organization personnel should be aware that when they use organization web and e-mail services, they are protected by the organization's web and e-mail protection preventive and detective controls. These controls may limit the sites they can visit or the content they can download. Some specific aspects of the organization's web and e-mail protection to consider are as follows.

Web Filtering and Decryption

These security protections involve intercepting web browsing network traffic from organization computers and scanning that traffic for potentially malicious patterns. Such patterns might include malware downloads, data exfiltration, or command-and-control traffic. Web filters can enforce an organization's "acceptable use policies" governing how employees browse or use the internet. Advanced web filtering can intercept encrypted connections to secure web sites, which can be helpful against advanced attackers who secure their communications. Organizations generally provide web filtering protection to personnel connecting to networks within their facilities, although protections may be provided when users remotely connect as well.

Organization personnel should be aware that web filtering and decryption capabilities are intended to protect their web browsing on organization computers, block communications to prohibited web sites, and to investigate connections to questionable websites. There should be no expectation of privacy when surfing the web from organization computers.

E-Mail Filtering, Phishing, and Spear Phishing Defenses

These security measures are intended to reduce the amount of unwanted e-mail, malicious attachments, and phishing and spear phishing attacks. Studies have found that 90% of malware arrives via e-mail.[5] E-mail filtering

5 "2019 Data Breach Investigations Report," Verizon, May, 2019.

and defenses can block many types of cyberattacks and significantly reduce the organization's cybersecurity risk. However, advanced phishing techniques can be difficult to block, and attackers are finding new ways to defeat e-mail filtering every day. Organizations should anticipate that some malicious e-mail will get inside the organization. To address this reality, e-mail filtering can be configured to work together with web filtering, so the two protections work together. For example, when personnel click on e-mail links and get re-directed to malicious web sites, web filtering may recognize the sites as malicious and block them from downloading.

Organization personnel should be aware that e-mail filtering, phishing, and spear phishing defenses are designed to protect the organization from inbound attacks coming through e-mail, and that e-mail remains the most common vector for cyberattackers to get into the organization. Personnel should be tolerant when legitimate messages get incorrectly tagged as malicious, and should adhere to organization processes for investigating and reporting malicious e-mails. Finally, personnel should remember that no amount of filtering is 100% effective, and that spam, phishing, and spear phishing messages are going to sometimes get through. Everyone needs to pay attention to the messages they receive, and be careful opening attachments or clicking on links.

E-Mail Nonrepudiation and Encryption

These security technologies enable organization users to digitally sign e-mails to prove that the e-mails originated from the organization and are legitimate. They can also encrypt organization e-mails to make them almost impossible to intercept and read. These protections enable organizations to use e-mail to transmit sensitive, confidential, or protected customer information such as Health Insurance Portability and Accountability Act (HIPAA) data, personally identifiable information (PII), or financial data.

Organization personnel should be aware that e-mail nonrepudiation and encryption capabilities can enable them to send strongly protected e-mails inside and outside the organization. When exchanged outside the organization, signed and encrypted e-mails provide strong protection against many types of e-mail attacks and fraudulent messages. Organization policies may require that these capabilities be used for certain types of e-mail messaging, such as company-wide directives or regulated confidential correspondence.

Remote Access to Organization IT Resources Cyber Awareness

This cyber awareness topic involves cyber protections for personnel accessing organization IT systems remotely, such as employees on the road or working from home. It may also apply to remote third-party users, such as contractors or business partners. These users need remote access to organization resources, such as IT resources, capabilities, or data. While traveling employees have been an organization norm for decades, employees working from home has increased significantly over the past two decades and is now commonplace and will be even more so going forward due to impact of the coronavirus pandemic of 2020.

Regular remote work can place unique strains on employees and organization IT resources alike. Successful remote worker arrangements can require (1) flexible IT environments with around-the-clock technical support, (2) employees to be familiar with an increasing number of digital collaboration and communication tools, (3) increased cybersecurity protections such as multifactor authentication, (4) up-to-date security policies and processes, (5) virtual office collaboration arrangements, and (6) increased cybersecurity awareness and training.

Organization personnel should be aware that when they use organization remote access services, they are protected by the organization's remote access preventive and detective controls. Some specific aspects of the organization's remote access security protections to consider are briefly described in this section.

Virtual Private Network (VPN), Secure Sockets Layer (SSL), and Internet Protocol Security (IPSec)

These security capabilities provide the ability to extend an organization's internal networking resources to external or remote users in a secure manner.[6] VPN is a network security technology that involves creating an encrypted tunnel from one host computer to another over an untrusted network. This encrypted tunnel is used to connect the networks at both ends so they are "virtually" connected and "private" from the network in between.

6 Note that modern implementations of SSL actually use the Transport Layer Security (TLS) protocol, which is a different protocol derived from SSL. TLS was designed to address issues and vulnerabilities in the SSL protocol, and the actual SSL protocols are obsolete and should not be used. However, the term "SSL" has stuck, and is usually used to refer to both protocols, interchangeably.

SSL and IPSec are commonly used protocols for implementing organization VPNs. SSL provides an open-standard encryption capability designed for client-server communication, and is also used for securing connections to web sites for online banking, stock brokerage, web e-mail, and other purposes. IPSec provides high-speed authentication and encryption for online communication traffic, although it has been largely superseded by SSL in most VPN implementations. Both protocols may be combined with multifactor authentication to securely identify users before they are allowed to communicate over a secure channel.

Organization personnel should be aware that VPN, SSL, and IPSec protocols will likely be required to protect connections to organization web sites, e-mail, networks, and other applications. Personnel should look for "lock icons" in web browsers and other tools indicating secure connections when they connect remotely to the organization. Personnel should treat insecure connections as suspicious signs that they are being tricked or their computers have been hacked.

Virtual Desktop

This capability, sometimes known as thin clients, involves using virtualization to run a desktop computer operating system on a server within the organization's datacenter or cloud service. Remote users then connect to that "virtual desktop" computer from their personal device or remote location, using a special application, web browser, or specialized terminal appliance. Some organizations even use virtual desktops in an office environment, so IT personnel do not have to go desk to desk to help with personal computer issues. Virtual desktops can deliver multiple advantages, including central control of desktop computing configurations, strict control over organizational data, and high-performance computing. Perhaps most importantly, virtual desktops enable users to securely access their organizational data and files over the internet, regardless of the users' physical location or computing devices.

Organization personnel should be aware of how a virtual desktop can enable them to work securely from personal or insecure computers, if this service is available. Personnel should be aware that virtual desktops can allow them to access organization data without having to download it to the local computer, which can be a powerful protection against leakage of sensitive data. However, they should also be aware that even though the data is staying on the virtual desktop server, local "screen scraper" malware can still see everything the user sees, and may be able to read some sensitive data through the virtual connection.

Mobile Device Management (MDM)

This security software provides a secure method to access the organization's e-mail, calendar, and contacts on personally owned mobile devices, such as smartphones or tablet computers. MDM protects organization data by establishing an encrypted container on the local device, and then using that container to store local copies of e-mail messages, calendar entries, contacts, file attachments, or other organizational data. The MDM software prevents secure data from being exchanged with insecure parts of the device, in effect creating an area reserved for organization data that is isolated and controlled by the organization. If there is an issue with the mobile device, the organization can remotely "wipe" or "remove" its data from the device without impacting the owner's personal data or applications.

Organization personnel should be aware of how MDM can protect their mobile devices connecting to organization e-mail, calendar, and other applications. They should understand that while MDM keeps organization data secure, it does not make their devices impregnable or invulnerable to cyberattack or compromise. They should be aware that the organization's MDM capability, in addition to protecting organization data, can be used to remotely wipe their device to protect their personal data as well, in the event the device is lost or stolen. Just make sure it is securely backed up somewhere.

Cybersecurity Operations Cyber Awareness

This cyber awareness topic involves maintaining the organization's security on an ongoing basis and actively monitoring to detect incidents against the organization's IT environment. Cybersecurity operations includes a number of ongoing processes that are used to keep the organization's cyberdefenses operating properly. These processes include rogue device and network detection, system change detection, vulnerability scanning, patch management and deployment, and monitoring of system performance and security. Frequently, these functions are run out of a security operations center, or SOC. Sometimes, they may be performed by an external partner as part of a managed security service (MSS) or managed detection and response (MDR).

Organization personnel should be aware that when they are using the organization's IT resources, they are a part of the organization's cyberdefense posture and subject to its cybersecurity operations preventive, detective, and response controls. Some specific aspects of the organization's cybersecurity operations to consider are as follows.

Rogue Device and Network Detection

These operational capabilities involve the organization being able to detect when rogue, or unauthorized, devices are connected to organization networks. These devices may be personal computers, gaming devices, network-connected appliances, or additional networking components. Sometimes, users may create their own Wi-Fi hotspots or connect their own sub-networks to organizational networks. These actions can jeopardize organizational security by introducing components that are insecure, or by compromising the security and integrity of protected networks.

Organization personnel should be aware of the dangers of rogue devices and network connections, and be educated on organization policies regarding connecting personal or unauthorized devices to organization networks. Personnel should be informed that rogue devices may be detected and investigated, should they be connected to the organization's private networks.

System Change Detection

These operational capabilities involve the organization being able to detect when unauthorized changes are made to organization endpoints, servers, applications, services, or infrastructure. These capabilities are often implemented through scanners that establish known baselines of system configurations, and then periodically scan the systems to compare their configurations to the baselines. When authorized changes are made, the baselines are updated, but when unauthorized changes occur an alert is raised for investigation. This monitoring capability can detect suspicious changes that are not related to legitimate patching or system update activities. Unauthorized configuration changes can be strong indicators of attacker activity in organization IT systems.

Organization personnel should be aware that organization systems and applications may be monitored to detect unauthorized changes. Personnel who need to make changes need to go through proper change control and authorization processes, even if they have the access or permissions to simply make the changes. Although usually applied to system software and configurations, change detection can also be used to catch changes to sensitive data files, user permissions, and other data elements that should not be changed without authorization.

Vulnerability Scanning and Patch Management

These operational capabilities involve scanning organization networks, computers, servers, and devices for vulnerabilities, and then patching those vulnerabilities on a regular basis. Organizations should regularly scan their IT systems for known vulnerabilities, and then address those vulnerabilities in priority order. Critical vulnerabilities in internet-facing or security-critical systems may require immediate attention, while low-severity vulnerabilities in secondary systems may never get addressed. Minor vulnerabilities may be acceptable in secondary systems that are protected by other defenses like the network perimeter or cloud environment. Where possible, patches should be deployed in an automated fashion soon after they are released by the manufacturer. Even non-critical patches may be helpful in keeping organization software up to date according to software vendor guidance. Where patches address critical vulnerabilities, they may have to be deployed on an emergency basis.

Organization personnel should be aware that critical vulnerabilities can leave the entire organization open to cyberattack, and that new software vulnerabilities may be identified at any time. Organization IT systems may be regularly scanned for vulnerabilities, and organization IT personnel may have to deploy patches on short notice, especially when critical vulnerabilities arise. It is particularly important for internet-facing servers and personal computers to be kept up to date. Personnel should understand that when their endpoints are being updated, or when they are asked to reboot to install a patch, they need to treat the situation as one of organizational security, and perform the required actions as soon as practical.

Monitoring of System Performance and Security

These operational capabilities involve monitoring the organization's IT system performance and cybersecurity sensors. These measures can detect when operational anomalies occur that may be security-related, as well as cybersecurity alerts that may be indicative of cyberattacks. For example, operational monitoring may be able to detect when systems are working harder due to malware or ransomware, or have rebooted or crashed due to malicious activities. There are various tools to help analysts detect, diagnose, and resolve performance issues, and to identify if performance issues are related to hardware, software, or human activity. Similarly, network monitoring may be able to detect cyberattackers attempting to remove data files from the organization's servers, or

command and control connections from over the internet. Since potential security alerts can only be detected from systems that are monitored, having monitoring in place is the first step toward detecting cyberattacks when they occur.

Organization personnel should be aware that organization IT systems are monitored for their operational performance and cybersecurity. IT professionals should understand that connecting applications, servers, and other IT systems to organization monitoring systems is an important step in production deployment. Personnel should monitor their personal computers, and understand that symptoms like high processor usage, slow networking, and heavy storage use may be signs of malware or attack. Organization personnel should understand that they may be called upon to help investigate alerts raised by performance or security monitoring, and should make assisting with that investigation a high priority.

Security Operations Center

These operational capabilities involve bringing the organization's detection capabilities together into a security operations center, or SOC. In large organizations, the SOC may be a 24x7 operation staffed around the clock to detect and investigate cybersecurity incidents. In smaller organizations, it may be a single person or small team, or an external managed security service (MSS). The SOC will likely use log aggregation, along with security information and event management (SIEM) tools to help them perform their duties. SOC incident detection involves collecting events across the IT environment, analyzing those events for security alerts, cross-correlating event data across multiple streams, and performing analysis to separate incidents from false positives. SOC personnel may analyze incidents to identify attackers, direct defenses, and predict future attacker activities. While performing its cyberdefense duties, the SOC may use honeypots, honeynets, and honeytokens to mislead attackers and identify their tools, techniques, and procedures (TTPs).

Organization personnel should be aware of the presence of the SOC, if there is one, and know how to contact it to report a known or suspected cyber incident. Personnel should understand that the SOC is there to defend the enterprise, and that SOC staff may require their assistance to investigate an incident or perform a cyberattack response. SOC operations should be closely coordinated with other front-line IT services, like desktop support and the IT help desk, to help identify security incidents and coordinate incident response.

Incident Response Cyber Awareness

This cyber awareness topic involves an organization responding to cybersecurity incidents when monitoring reveals evidence of malicious activity in its IT systems. Unlike ongoing monitoring, incident response is event-driven and only occurs when monitoring reveals that an incident has actually occurred. When an incident response process is invoked, a number of activities need to occur in order to identify the activity, contain it, and ultimately remediate the breach and restore normal operations. Incident response also serves a strategic cyberdefense purpose by providing feedback to the major IT functions of architecture, engineering, and operations. Such feedback helps to identify weaknesses in organization security and provides short-term and long-term remediation advice to address those weaknesses.

Organization personnel should be aware that they may have a role to play in the incident response process, regardless of their position in the business. Cyber incidents can affect every area of the organization's business, and personnel should be prepared to support the incident response process, if they are asked. Some specific aspects of the organization's incident response process to consider are as follows.

Cyber Threat Awareness

This process involves being aware of the threats targeting the organization, and the different types of cyberattacks that may be targeting the organization's country, industry, or technology. *Are there major cyberattack campaigns coming from nation-states right now? Are ransomware campaigns targeting the organization's industry right now? Are attackers exploiting a new vulnerability in the organization's desktop operating systems, application platform, or mobile devices?* These are all factors that can affect the organization's cybersecurity status, due to increases (or decreases) in the active cyber threats. Threat intelligence feeds can provide organizations with information on the sources, types, techniques, and tools of likely cyberattacks. Organizations should select those threat intelligence sources that provide relevant, actionable intelligence to help indicate potential data breaches.

Organization personnel should be aware of the cyber threats against the organization, and the techniques attackers may be using to target the organization's people and technology. Many cyberattacks target organization employees through phishing and spear phishing campaigns, and by targeting user credentials

or remote access channels. Personnel should be aware that no role or position is safe from targeting, and that they should be ever vigilant.

Incident Detection, Investigation, and Forensics

This process involves the organization detecting and investigating cyber incidents, along with using available investigation and forensics tools to identify the computers, accounts, and network traffic involved in the cyberattack. Ideally, cyberattack detection and investigation should occur while the cyberattack is in-progress, although for most organizations this is the exception rather than the norm. When SOC personnel are investigating incidents, they will frequently use forensic tools that allow them to take "snapshots" of computers and their storage. These forensic tools permit detailed analysis of the running programs and stored software on the subject computers, and may be used even after the affected computer has been taken offline, rebooted, or re-imaged for re-use. Additional tools may allow investigators to investigate attacker network traffic, compromised user accounts, and unauthorized changes involved in the cyberattack. These tools can also be important if the investigated incident involves criminal activity, as good forensic tools include safeguards to support the handling and analysis of data in accordance with law enforcement procedures.

Organization personnel should be aware of the incident detection, investigation, and forensics process. Personnel should be aware that an incident investigation can involve any person, any account, any computer, and any network used in the organization. Personnel who are contacted by cyber investigators should be prepared to cooperate in the handling of their accounts, personal computers, mobile devices, and other IT equipment involved in the investigation. Personnel should also understand that incidents relating to criminal activity may require giving statements to organization legal counsel, external consultants, or government law enforcement staff.

Incident Response, Containment, and Recovery

This process involves supporting the organization's efforts to respond to a cyber incident, contain the cyber attacker, and ultimately recover from whatever damage that was done. The incident response process may involve considerable disruption to the organization's IT environment. For example, containing a rapidly moving cyberattacker may require disabling large numbers of user accounts,

entire datacenters of computers, or isolating the organization from the internet. Similarly, containing rapidly spreading malware may require actions as dramatic as isolating infected facilities, or even shutting down the entire network. Recovering from a cyberattack may require similarly drastic actions, including resetting every user's password, re-imaging large numbers of personal computers, or taking organization applications offline for an extended period of time.

Organization personnel should be aware of the incident response, containment, and recovery process, and understand that a fast-moving cyberattack scenario may require dramatic action to be taken, very quickly. It is possible that personnel may find they are locked out of the network, or their computer is disabled, in the name of a cyberattack response. They may also find that their personal organization computer needs to be confiscated and re-imaged, as part of a cyberattack response. Hopefully, the most important data was backed up.

Regulatory and Legal Coordination

This process involves interfacing with regulatory, legal, and law enforcement organizations as part of a cyber incident response. This process may include digital crime investigation, which follows prescribed procedures for identification, collection, analysis, safeguarding, and presentation of evidence to law enforcement and criminal courts. In a criminal investigation, chain of custody is very important, along with controls to ensure that evidence is not compromised or tampered with prior to presentation to law enforcement. If proper legal procedures are not followed, the organization may find its evidence is disqualified for consideration by law enforcement or the court, which could jeopardize the organization's legal position in a civil or criminal trial. Similarly, the organization must be aware of the regulatory impact of its cyber incidents. Cyber incidents regarding regulated data such as personal privacy data, healthcare data, or financial data, may require special handling and consideration. Organization legal departments may be involved, along with auditors, to ensure that regulatory disclosure and compliance requirements are satisfied.

Organization personnel should be aware of the regulatory and legal consequences of potential cyberattack incidents. Incidents affecting proprietary data, regulated data, or resulting in organizational or personal harm may have regulatory or criminal implications for the organization, as well as its people. Personnel should understand that when a cyber incident becomes a regulatory, legal, or criminal concern, the level of seriousness increases considerably. Personnel should understand they need to comply with organization guidance

and consult legal staff if they have questions. Some personnel may even want to retain their own legal counsel, if their actions (or inactions) were integral parts of the incident that occurred.

Operational Disruptions

This process involves understanding the operational disruptions that may come from a cyberattack, or the organization's response to the cyberattack as it seeks to protect itself and its IT systems from the attackers. Ransomware in particular has shown itself to be highly disruptive for victim organizations, but it is hardly the only type of operational disruption. As we saw with Saudi Aramco and Sony Pictures, attackers may seek to disrupt the organization's IT operations, without even demanding a ransom. Other cyberattacks have disrupted power generation, telecommunications, or even caused a blast furnace to malfunction.[7] Cyberattacks may cause all measure of disruptions to organization IT systems, and can affect isolated manufacturing or healthcare delivery networks, in addition to internet-connected business networks.

Organization personnel should be aware of the threat that cyberattacks can pose to the organization's operations, and understand that both cyberattacks, as well as the efforts to contain them, can result in significant disruptions to the organization's business operations. One should not underestimate the impact of IT or network outages, even on relatively low-technology manufacturing environments. Personnel should have backup paper-based procedures in case IT systems are not available, and should practice those procedures regularly in case a severe cyber incident should occur.

Physical Security and Personnel Protection Cyber Awareness

This cyber awareness topic involves protecting organizational data, the facilities where that data is located or accessed, and the trustworthiness of the people with access to the organization's data and sensitive information systems. This cyber awareness topic includes protecting against hackers who attempt to gain access to organization facilities or personnel, and then use that access to target organization networks, computers, applications, sensitive data, and operational

7 Cyberattack against a German steel mill in 2014, as reported by the German Federal Office for Information Security.

processes. While information security involves placing controls and safeguards around information systems, the reality is that physical access can bypass many of the cybersecurity protections that organizations operate. Organization cybersecurity and industrial security personnel should regularly coordinate their activities so physical security and cybersecurity can work together as complementary practices protecting the organization and its business interests.

Organization personnel should be aware that when they are in organization facilities, they are protected by the organization's physical security and personnel protection. They need to abide by the organization's policies for personnel security, background checks, and industrial security incident reporting. Some specific aspects of the organization's physical security and personnel protection to consider are as follows.

Facilities Protection

Facilities have their own set of challenges with regard to human made threats like intrusion, theft, or sabotage, as well as natural threats like fire, flood, earthquake, tornado, or hurricane. A comprehensive facilities protection plan should include consideration of neighborhood location, local crime rates, and area natural disaster ratings. It should also consider proximity to fire, police, and medical centers, connectivity to major highways, and support from utilities such as power, water, and sewer. Finally, it should consider the information assets of the organization that can be accessed from the facility, either locally or remotely using trusted network connections. Trusted facilities can frequently access sensitive organization information systems, via secure terminals, trusted network connections, or stored user credentials.

Organization personnel should be aware of the importance of protecting organization facilities, and the information systems they can access. Personnel should understand that even minor facilities, if they have access to organization networks, can be the source of significant cybersecurity breaches if they are compromised and give network access to cyberattackers.

Physical Access Controls and Security Monitoring

These protections defend against malicious actors gaining access to a protected facility, or detect such access should attackers get past the physical protections. Physical access control systems may be deployed to manage and log the flow of visitors and employees into and out of the facility over the course of the

workday. Personnel protection may include access badges, restricted areas, security screening, and metal detectors. Many organizations are weapon-free and drug-free zones, subject to local laws and regulations, and may preform checks for contraband as part of their access control process. Physical security monitoring capabilities can include access control monitoring systems, closed-circuit TVs, physical intrusion detection systems, proximity sensors, and entryway access logs. In addition, electronic and manual locks, fences, lighting, and guards can play important roles in the organization's physical security posture and ability to detect and respond to physical intrusions.

Organization personnel should be aware of the physical access controls and security monitoring protecting the facilities where they work. They should understand that physical security is often more of a deterrent than an actual protection, and that determined attackers will find ways into organization facilities. Therefore, personnel must be diligent about security measures like checking for badges, guarding against tailgating (where an attacker follows an employee into a building), and challenging unknown and unbadged personnel. Organization personnel should be aware of physical security policies, and their responsibilities for upholding those policies to protect the safety of the organization's facilities, its personnel, and the information assets they can access.

Personnel Security, Background Checks, and Drug Screening

These security screening processes are important parts of organization protection, particularly when sensitive or regulated data is being handled by organization personnel. Malicious or negligent employees or other insiders can cause immeasurable and possibly irreparable harm when things go wrong. Regulations may require significant background checks for certain positions of trust or public safety. Background checks are often performed in the first phase of employee engagement during onboarding, and can include drug testing, verification of employment or education, and checks of internet or social media reputation. Often the recruiter, hiring manager, and human resources representatives are involved in onboarding new employees and performing such background checks.

Organization personnel should be aware of the personnel security, background checks, and drug screening required for their employment position. They should understand that some personnel security requirements may be based on regulations or contract obligations, while other security requirements may simply be organizational policy or guidelines. Personnel should be aware that such checks are an important part of establishing and maintaining

organizational trust, and are not intended to be impositions on personal privacy. The organization has to make a determination somehow, and screening is designed to identify behaviors that place personnel at higher risks for trust issues, based on organizational experience. In addition, personnel need to be aware that the organization may need to conduct regular follow-up reviews of criminal activity, financial health, or drug testing, to make sure personnel remain trustworthy. Organization trust is never a one-time event, and criminal activity by employees may become grounds for dismissal or prosecution.

Industrial Security Incident Detection, Investigation, and Reporting

These security functions are important components of an organization's industrial security program, and align directly with their cybersecurity counterparts. The organization may be required to perform specific handling of industrial security incidents for regulatory compliance, law enforcement coordination, or to meet other business objectives. Other business objectives might include reducing theft losses, preventing crime, and protecting the safety of employees, customers, or guests. Employees, partners, service providers, and vendors may be required to report certain types of security incidents, such as accidents, injuries, or suspected criminal activity. Under certain circumstances, such reporting requirements may extend to customers. Additional reporting requirements may include personal events such as international travel, criminal arrests, or workplace accidents.

Organization personnel should be aware of the organization's obligations and requirements for identifying security incidents, investigating security incidents, and reporting them both internally and with external parties. Management personnel should have clear guidance on which incidents require reporting, and the channels and formats for delivering such reports. Line personnel should understand the differences between cyber incidents and industrial security incidents, and the appropriate reporting channels for both. All personnel should understand their responsibilities to support incident investigation and reporting, and make such tasks a high priority when they are required.

Business Continuity and Disaster Recovery Cyber Awareness

This cyber awareness topic involves planning, preparation, and recovery activities to help ensure that an organization can maintain essential functions during and after disruptions, security incidents, or disasters. Disruptions might include

power outages, critical business system failures, or failures of IT technologies. Security incidents might include cyber or physical incidents compromising the confidentiality, integrity, or availability of organization information. Disasters might include fires, hurricanes, or industrial accidents. Business continuity and disaster recovery planning can involve considerable activities preparing the organization for how it might continue in the face of natural, humanmade, or criminal disaster situations.

Organization personnel should be aware that they may have a role to play in the organization's business continuity and disaster recovery process, regardless of their position in the business. Disasters, whether they are natural, criminal, or IT in nature, can affect every area of the organization's business. Personnel should be prepared to support the business continuity and disaster recovery process, if they are asked. Some specific aspects of organizational business continuity and disaster recovery to consider are as follows.

Contingency and Disaster Recovery Planning

This practice area involves developing plans and procedures for continuing to deliver business services while primary facilities, IT systems, or personnel are unavailable. It also includes developing plans for recovering normal business operations after a disaster has occurred. An organization should plan for various adversity scenarios that might include natural or man-made disasters, loss of facilities, loss of personnel, or loss of connectivity. Contingency plans should focus on keeping the most critical business functions operational after things have gone wrong, while simultaneously dealing with the underlying problems, protecting the organization's people, and reducing the collateral damage. Some planning may consider potential effects on the organization's reputation or strategic impacts on its business or mission, as well as considering third-parties that support the organization. Disaster recovery planning should include steps to restore IT systems, business applications, and critical data after a disaster has occurred. Planning should include procedures for restoring services after potentially dramatic losses of facilities, personnel, or IT systems.

Organization personnel should be aware of the types of natural, humanmade, and failure-based disasters that may befall the organization. They should understand how the organization may have to activate contingency capabilities, or activate alternate facilities or locations. They should understand the business's operational priorities, and what needs to be done first when there is not enough time or resources to do everything. They need to understand how

the organization may transition to contingency operations, and how it might transition back to normal operations, after the disaster is resolved.

Data Replication, Backups, and Off-Site Storage

This practice area involves having IT capabilities in place to protect against failures of IT systems, facilities, or networks. These capabilities replicate critical data to multiple locations so that even if the primary systems or data are lost, critical information can still be recovered and made available to organization personnel. Data protection may include replicating data from primary to backup systems, backing up data on a set schedule, and copying data to storage locations away from the primary facilities. These techniques, along with supporting processes for servers, applications, and networks, make it possible for the organization to keep critical business applications and processes going, even after failures have occurred.

Organization personnel should be aware of the organization's strategy for replicating data, backing up data, and using off-site storage to protect against failure scenarios. They should understand the business impacts of the organization having to switch over to backup applications, activate backup facilities, or restore critical data from archives. They should understand that some of these scenarios might result in data loss or missed transactions. In these cases, the most recent transactions or activities may have to be manually reconstructed. Personnel should know the procedures for using paper backups, local records, or written notes to reconstruct lost transactions.

Devastating Cyberattacks

This practice area involves preparing the organization for the possible impact of devastating cyberattacks. Devastating cyberattacks might include widespread ransomware infection, destruction of IT systems, or physical damage to facilities or equipment. Some scenarios may even result in physical harm to personnel, such as with industrial or healthcare environments. While disaster recovery planning may cover such scenarios in general, the organization should give special attention to specific cyberattack scenarios, and understand that deliberate cyberattackers may go out of their way to destroy not only the organization's operational capabilities, but its recovery capabilities. Plans for these situations can go a long way toward being prepared for the most

dangerous cyberattack scenarios. The organization should consider the following questions in conducting its devastating cyberattack preparation.

- *Does the organization have archived backups that are isolated and known to be good?*
- *Does the organization have snapshots of its IT system and application configurations that are completely separate from production systems, and can be used to recover its servers and applications?*
- *Is critical operational data stored on personal computers that might be lost in the event of a widespread malware outbreak or cyberattack?*
- *Does the organization have procedures for an emergency shutdown of its IT systems to stop a fast-moving malware outbreak or cyberattack?*

Organization personnel should be aware of the possibility of devastating cyberattacks against the organization, and how devastating cyberattacks can be different from normal operational failures, accidents, or natural disasters. They should be aware of the cyber threats against the organization, particularly if it has run afoul of known cyberattack groups, nation-state adversaries, or if its business industry is a known target for potential devastating cyberattacks. Personnel should be aware of how the organization may have to respond against a devastating cyberattack, and their responsibilities to support such a response should it become necessary.

Business Continuity and Disaster Recovery Exercises

This practice area involves the organization conducting regular exercises to practice its business continuity and disaster recovery processes. This practice might include tabletop exercises, contingency operation, and practice recovery drills. Tabletop exercises might involve organization executives and management, various disaster scenarios, the organization's responses, and different departments' responsibilities to facilitate contingency operations and recovery processes. Contingency operations may include the organization switching over to backup IT systems, or backup manual procedures, for a period of time to make sure backups work and everyone knows what to do. Recovery drills might include practicing the recovery of IT systems or operational processes from archives, or offline backup copies. Exercises like these give the organization opportunities to practice its business continuity and disaster recovery processes, and to capture valuable lessons learned that may be applied if the real thing ever comes to pass.

Organization personnel should be aware of the organization's processes for conducting business continuity and disaster recovery exercises, and their role in participating in such exercises when they occur. Personnel should be involved in exercises where possible, so everyone has experience operating "in contingency mode." Through this type of experience, personnel can understand how the organization might continue to operate, even when highly impaired by a disaster situation.

Chapter 11
Cyber Training

To achieve organizational cyber awareness, an organization must deliver awareness training to its staff. Ever-present and evolving cyber threats require awareness training that is adapted to the latest threats, the needs of the organization, and the roles of the personnel. Training can include presentations given at lunch time; online, on-demand training describing various security issues; periodic training exercises; and seminars. However, such training should be more than once-a-year or twice-a-year occurrences, or a handful of meetings and training exercises. To endure over time, cyber training and the resulting best practices should be an integral part of an organization's culture.

Organizational cyber training needs include "basic" training that should be delivered to everyone, as well as "role-based" training tailored to the specific responsibilities of specific groups of staff or personnel. Training should be developed considering how the latest cyber threats affect the day-to-day responsibilities of organization personnel, so such personnel can be continually aware of the changing cybersecurity landscape. Simply stated, an organization needs to decide what cyber training is required to support its unique goals and mission. The question is: *What cyber training will impact day-to-day, mid-term, and long-term staff behavior to help the organization protect itself against both external and internal cyberattacks?*

As depicted in Figure 11.1, cyber training is about bringing the organization's cyber awareness topics to the attention of the stakeholder communities that need to be cyber-aware.

Since cyber threats are ever-present, it is critical that an organization design its cyber training program to present those threats to its people in an approachable and accessible fashion. Depending upon an organization's size, complexity, and day-to-day operations, its training plan can include a wide range of topics. For example, an organization's training plan may include the following *representative* cybersecurity topics:

- Common threats, such as phishing attacks aimed at an organization's general population.
- Less-common threats, such as spear phishing aimed at senior executives or administrators.
- Evolving or new cyber threats to help keep the organization cyber aware of the latest threats.

https://doi.org/10.1515/9781501506529-011

- Core concepts such as creating strong passwords, recognizing suspicious e-mails, and knowing who to notify about malicious websites or potential insider threats.
- Cybersecurity functional areas, processes, policies, procedures, guidelines, and standards.
- Simulated but realistic cyberattack scenarios, such as organization-sponsored phishing attacks designed to prompt desired security behavior from employees.
- Physical security controls, such as physical access control devices and security guards that protect the security of the organization's facilities.
- Physical environmental controls, such as fire suppression systems and sprinkler systems, important to personnel safety.
- Feedback mechanisms, public and anonymous, to allow employees to provide improvement suggestions on training methods and techniques.

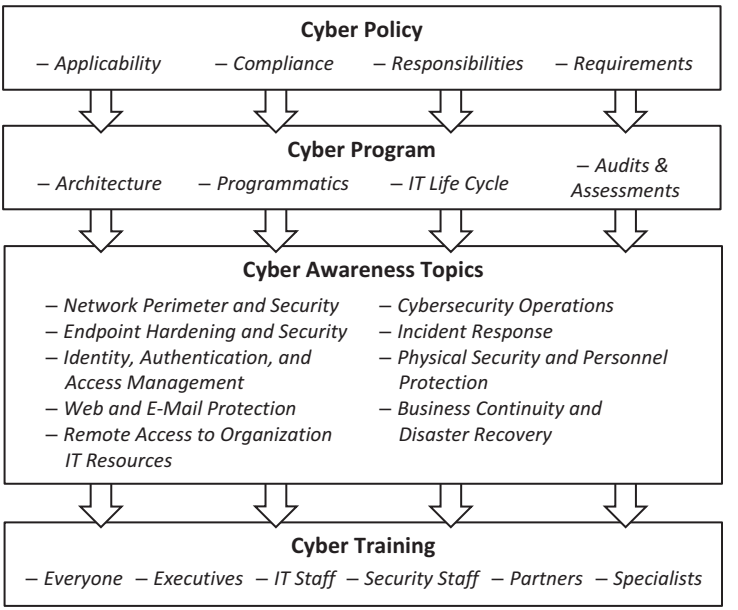


Figure 11.1: Cyber training brings the organization's cyber awareness topics to the different communities of people who should be cyber-aware.

Regardless of the training content, senior executives should be involved in creating messaging about the organization's cyber training program. This involvement helps set context and emphasizes the importance of cybersecurity

and the organization's rationale for operating its cybersecurity program. Executives can stress the importance of aligning cyber training to the organization's *cyber policy*.[1]

As shown in Figure 11.1, cyber policy establishes the foundation upon which an organization's cybersecurity program is built, and represents a contract between the organization and its cybersecurity practice. Policy directs what is to be protected and to what degree, as well as specifying consequences for violations. Policy then drives the cyberdefenses in the organization's cybersecurity program, on one hand, and the topics for the organization's cybersecurity awareness, on the other hand.

Cyber training should provide the knowledge, skills, and abilities (KSAs) needed to build and maintain the organization's cyberdefenses. To aid in developing such training, the National Institute of Standards and Technology (NIST) led the development of the National Initiative for Cybersecurity Education (NICE). This initiative defines a cybersecurity workforce as "work roles that have an impact on an organization's ability to protect its data, systems, and operations."[2] These work roles include position descriptions for both technical and non-technical staff. An organization can use the NICE Framework "to define or provide guidance on different aspects of workforce development, planning, training, and education." NICE is a very useful resource when designing a cyber training program, and has been used to design industry-accepted cyber certifications.

People properly handing sensitive information is essential to the success of an organization's cybersecurity posture.

A robust cybersecurity training program includes training that is tailored to the needs of the organization's stakeholders. Some of the types of cyber training the organization may wish to conduct are as follows:

- **Cyber Training for Everyone.** This training might be for everyone using organization IT systems. This training would also serve as a baseline for specialized awareness training the organization might chose to deliver to specific sub-groups like executives or IT staff.

---

1 See Appendix C, "Example Cyber Policy" for a detailed example of such a policy.

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

- **Cyber Training for Executives.** This training might be for executives, such as the chief executive officer (CEO), chief financial officer (CFO), chief information officer (CIO), chief information security officer (CISO), and other organization senior management. Executive cyber training might include risks associated with specific attacks targeting executives, such as spear phishing, whaling, bank attacks, and espionage.
- **Cyber Training for IT Staff.** This training might be for IT personnel who have administrative access to organization IT systems and services during their life cycles. IT staff training might include privileged accounts, incident detection and investigation, and supporting remediation efforts.
- **Cyber Training for Security Staff.** This training might be for security and cybersecurity personnel who have higher standards for performance because they set the example of required cyber behavior. Security staff training might include risk management, security operations center (SOC), cyber incident response team (CIRT), and compliance activities.
- **Cyber Training for Partners.** This training might be for partners, contractors, and other third parties. Partner training might include topics such as: custom software development, contract agreements, required security training, and contract compliance.
- **Cyber Training for Specialists.** This training would be for people in specialized roles not already discussed or roles that emerge due to unique business requirements. Specialist training might include niche topics such as handling the internet of things (IoT), mobile technologies, or securing programmable logic arrays (PLAs).

Cyber training may be standalone training, or it may be integrated with other training on general security practices, business risks, or regulatory compliance. Cyber training should help employees be aware of the organization's cyber risks, how the organization can mitigate those risks, and the employees' responsibilities regarding those mitigations. The following sections contain specific ideas for developing cyber training tailored for the needs of the organization's different stakeholder communities.

Cyber Training for Everyone

This training might be for everyone using organization IT systems. This training would also serve as a baseline for specialized awareness training the organization might choose to deliver to specific sub-groups like executives or IT staff. This training includes what employees need to do to comply with the organization cyber

policy. It instructs employees on what they need to do to protect organization data and information systems from unauthorized access, inappropriate disclosure, or compromise. It also instructs employees on how to respond to potential security incidents.

Cyber training topics for everyone may include information on the organization's security policy, evolving security threats, online scams, and IT basics regarding e-mail, social media, and collaboration tool usage. Training topics may address the following representative questions to help employees protect themselves and their workplace:

- *Who might attack my organization?*
- *Why would they attack us?*
- *How often would they attack us?*
- *What might the cyberattackers want?*
- *How can I make myself less vulnerable to cyberattackers?*
- *What are the signs that my organization IT devices (e.g., computer or smartphone) might be compromised?*
- *What should I do when I think my organization devices have been compromised?*
- *What are some common cybersecurity attacks? How might I recognize them?*
- *What would cyberattackers consider valuable?*
- *How can I secure my computer?*
- *How can I secure my applications?*
- *How can I create "strong" passwords that comply with my organization's policy and are resistant to attack?*
- *How might cyberattackers get my passwords or account credentials?*
- *How can I protect my passwords and other account credentials?*
- *How can I tell that my web browsing is secure?*
- *What are some characteristics of malicious websites?*
- *What is malvertising?*
- *Are all pop-up windows malicious?*
- *How can I download software safely?*
- *How can I protect my e-mail account from unauthorized access?*
- *How can I recognize malicious e-mail?*
- *What are phishing, spear phishing, and online scams? How can I recognize these cyber threats?*
- *What are counterfeit e-mails and how can I guard against them?*
- *How can I protect myself against unsolicited phone calls?*
- *How can I safely use social media?*
- *How can I protect myself when on business travel?*

- *Can I download applications from the internet onto my organization-provided computer or smartphone?*
- *What is multifactor authentication and when should I use it?*

Organization training for everyone should cover topics like these in a comprehensive but easy-to-understand fashion. Training should include periodic recertification, along with outreach to keep employees and other personnel apprised of the latest threats and cybersecurity current events. Employees should be required to complete policy-required security training periodically to help protect the organization's IT equipment, access credentials, and sensitive data.

Cyber Training for Executives

This training might be for executives, such as the chief executive officer (CEO), chief financial officer (CFO), chief information officer (CIO), chief information security officer (CISO), and other organization senior management. Executive cyber training might include risks associated with specific attacks targeting executives, such as spear phishing, whaling, bank attacks, and espionage.

Executives often have access to privileged and regulated information that is significantly more sensitive than information typical employees see. Compromise of an executive computer or account can have catastrophic consequences, including the draining of bank accounts or widespread destruction of organization IT systems. Consequently, executives should receive additional training on cyber threats and defenses against attacks targeting them. Executives should be aware of the risks associated with their roles, and the additional protections that may be required to protect them, their computers, and organization accounts. They should also be aware of specific attacks that target executives. Such training might include the following:

Spear Phishing

While phishing involves e-mails sent to a wide range of users, spear phishing involves highly targeted phishing e-mails that target specific individuals within an organization. These spear phishing e-mails might appear to come from people who are known by the targeted individuals. Attackers may use data gathered from social media sites to personalize the e-mails with the individual's name, information about other people within the organization, content from

organizational documents, or even business client particulars. This personalization of the phishing e-mails can dramatically increase the likelihood that the attack will succeed in tricking its victims to install malware, reveal credentials, or disclose other information. These e-mails might contain links to malicious websites, ask the individual to call a fraudulent call center, or have infected or malicious documents or programs attached to them.

Whaling

If spear phishing is targeted at executives in general, whaling e-mail messages are even more highly personalized and designed to be even more targeted. To trick senior executives, like the CEO or CFO, whaling attacks might be designed to come from other executives in the organization, professional connections, or family members. Since whaling e-mails are highly personalized and targeted, they can be very difficult to detect. One common whaling technique is for the cyberattackers to steal money from the organization by getting the individual to authorize a wire-transfer to the attacker. This attack technique is also known as business e-mail compromise. Sometimes the attackers might spoof or falsify the CEO's identity to direct employees to carry out the fraudulent financial transfer on the CEO's behalf.

Bank Attacks

Similar to whaling attacks, cyberattacks against organization bank accounts can originate internally or externally. Cyberattackers can gather enough personal and confidential data via social media (e.g., Facebook, Twitter) so they can impersonate a senior executive or manager. Then, the attackers direct employees to wire-transfer money to an account controlled by the attackers. Alternatively, the attackers may e-mail a financial institution that the organization uses and try to direct the institution to send money to a specific account. If the attackers can impersonate the organization e-mail addresses, these requests might appear to be legitimate. Attackers may also hijack an employee's confidential information used to access the organization's financial accounts, and attempt to use that information to access and steal funds. Unfortunately, organizations do not have the same fraud protections as individual consumers, so stolen funds might not be recoverable. To counter these possibilities, organizations may need to get insurance to replace stolen funds, should bank attack fraud occur.

Espionage and Export Control

Espionage is the act of clandestinely acquiring sensitive, confidential, or secret information without consent of the entity (e.g., government, organization, individual) that has such information. Governments conduct espionage (a.k.a. spying) for political, military, or economic reasons. Organizations might conduct espionage to obtain competitor trade secrets, intellectual property, financial information, and planning documentation. While espionage is often illegal, such crimes can be hard to detect, difficult to prosecute, and almost impossible to prove.

Senior executives are often espionage targets, particularly when traveling in a foreign country. Executives, and the people traveling with them, need to safeguard personal and organization travel documents, and electronic devices they take with them. Travelers should be cautious about sensitive data by encrypting hard drives and mobile media. They should consider taking "burner" phones that allow for anonymous phone numbers and easy disposal. Travelers should also be cautious about their conversations. Proprietary organization information such as its negotiating strategy should not be discussed in public areas.

Business travelers should also be aware of international laws and politics. For example, different countries have different rules regarding data handling, merchandise for demonstration or samples, prescription drugs, and controlled substances. Travelers may have difficulty with government laws and regulations, especially if they work for a government contractor, do government business, or have a security clearance issued by their government. In the United States, some of the regulations governing international travel include the International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR). Briefly restated, these regulations govern data taken outside the country, or made available to foreigners in some way (such as over the internet).

If travelers are in a business that handles export-controlled data or highly proprietary commercial data, they should know if such information is on their computers, removable media, or mobile devices. Encryption does not necessarily protect data from export, and just taking a device with export-controlled data on it outside of the country may constitute export. This can be true even if the travelers do not intend to leave it there. If travelers are in doubt about their devices containing ITAR/EAR information, they should check with their IT departments and instead, travel with separate "clean" devices that have never contained export-controlled data.

Cyber Training for IT Staff

This training might be for IT personnel who have administrative access to organization IT systems and services during their life cycles. IT staff training might include privileged accounts, incident detection and investigation, and supporting remediation efforts. This training should be focused on aspects of the organization's cybersecurity that affect its IT systems, and would be of interest to IT system personnel. These areas might include topics of identity and access management, cryptography, and application security, to name a few.

There are many ways to structure the IT organization and perform IT functions. Based on IT management frameworks such as Information Technology Infrastructure Library (ITIL), there are typically four major functions in an organization's IT department, under the chief information officer (CIO):

- **Strategy and IT Architecture** is responsible for coordinating the other IT departments to align the organization's technology with business functions. This alignment is accomplished, in part, through multi-year strategic planning, prioritization of investments, and management of strategic vendor and technology relationships.
- **IT Engineering** is responsible for designing, deploying, maintaining, and retiring organization technologies. This function includes translating business and technical requirements into practical solutions that work, are cost-effective, and can be maintained by the organization's IT operations staff.
- **IT Operations** is responsible for operating IT technologies efficiently and cost-effectively according to the organization's agreed-upon performance measures, such as service level agreements (SLAs).
- **IT Security** is responsible for managing risk, operating security controls and services, responding to cybersecurity incidents, and collecting evidence that the security controls and policies are operating as intended. While it is part of the ITIL framework, organizations may also want to treat IT security as a separate practice area for the purposes of cybersecurity training.

IT personnel maintain the organization's IT systems and services throughout their life cycles. Usually, they perform such tasks as *privileged users*, using *privileged accounts* to manage the organization's IT systems. NIST defines a *privileged user* as "a user that is authorized [by the organization] (and therefore, trusted) to perform security-relevant functions that ordinary users are

not authorized to perform."[3] For example, a systems administrator is usually a privileged user who provides the management of sensitive organization systems, services, and data.

NIST also defines a *privileged account* as "an information system account with authorizations of a privileged user." A privileged account is also known as an "admin account." Many privileged accounts can exist within an organization and need to be continuously protected, managed, and monitored. If malicious actors compromise such accounts, they can gain significant access to and control of organization data and information systems. The resulting damage to the organization could be catastrophic.

In addition to handling privileged accounts, organization IT personnel will need to be involved in dealing with cyber incidents. A security incident can originate inside the organization (insider threat), in external entities, or in the surrounding environment. Figure 11.2 depicts an example of the steps involved in an organization responding to a security incident.[4]

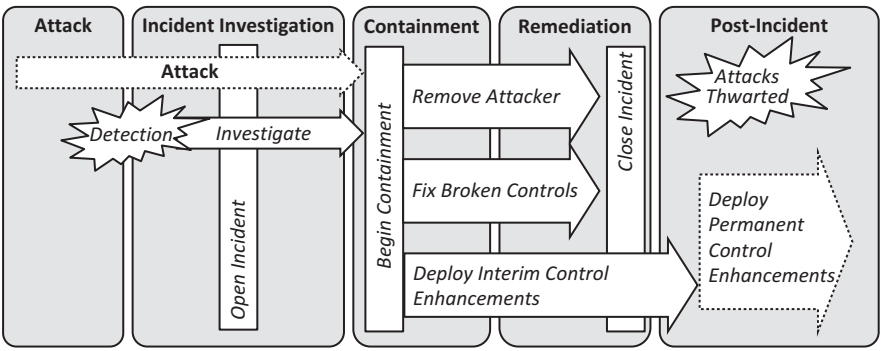


Figure 11.2: This notional cyber incident response process includes the initial incident investigation, containment, remediation, and deployment of permanent control enhancements to prevent a recurrence.

3 Joint Task Force for Transformation Initiative. "Security and Privacy Controls for Federal Information Systems and Organizations," National Institute of Standards and Technology (NIST): Special Publication 800-43 Revision 4, April 2013 (includes updates as of 01-23-2015).
4 Adapted from Donaldson, Scott E., Siegel, Stanley G., Williams. Chris K., and Aslam, Abdul. *Enterprise Cybersecurity*, New York: Apress, 2015.

The notional cyber incident response process consists of the following high-level activities:

- **Attack**. The incident starts with an attack and it may be as simple as a computer getting infected with a virus, or it may be an elaborate, multi-phase attack by cyber intelligence agents working from another country.
- **Incident Investigation**. After the attack is detected, defenders have an opportunity to begin responding with a preliminary investigation to filter out false positives. Corroborating evidence is collected to verify that the sensor reported an active attack. Once the attack is verified, the defenders formally start the organization's incident response process.
- **Containment**. After the incident is investigated and the extent of the attack is understood, the organization begins containing the attack. The response objectives include removing the attacker from the organization, fixing broken cybersecurity controls, and deploying interim control enhancements. These security steps should make it more difficult for the cyberattacker to get in again, or should detect if the cyberattacker succeeds in getting in again.
- **Remediation**. After the cyberattacker is contained, the defenders remediate the damage that was done, rebuild affected systems, clean up defaced web sites, and restore the organization back to normal operation. At the conclusion of remediation, the organization formally closes out the incident.
- **Post-Incident**. After the initial incident is remediated, follow-on attacks by the same attacker using the same tools, techniques, and procedures (TTPs) should be thwarted, or at least rapidly detected and defeated. Additional security controls deployed as a result of the attack may lead to long-term permanent security enhancements or strengthened controls.

The cyber incident process is often led by a security operations center (SOC) that works with engineering and operations to investigate and resolve incidents, and report the incident response status and business impact to management. When an incident is identified, the SOC takes charge of the incident and "pulls in" appropriate resources from elsewhere in IT and the organization to investigate and remediate the situation.

To support an effective incident response, the organization's IT staff, regardless of department, all need to be trained on their incident roles, responsibilities, and procedures. Business and non-IT staff may also have a role to play in the incident response process. The organization's basic training for everyone will need to include guidance on how to recognize and report potential security incidents and suspected malicious behavior. IT-specific training then builds upon that foundation to include specific guidance on the handling of privileged accounts, protection of IT applications, and support for the cyber incident response process.

Cyber Training for Security Staff

This training might be for security and cybersecurity personnel who have higher standards for performance because they set the example of required cyber behavior. Security staff training might include risk management, security operations center (SOC), cyber incident response team (CIRT), and compliance activities. This training would be tailored for security personnel's assigned security roles, responsibilities, and the information systems they are authorized to access. There are a number of IT security functions that typically report to a chief information security officer (CISO):

- **Risk Management** involves evaluating assets, vulnerabilities, threats, and risks; defining policies to manage those risks; and engaging with IT projects to identify and manage risks related to organization changes. This function may include security engineering to design, deploy, and integrate security solutions that support the organization's cyberdefenses.
- **Security Operations Center (SOC)** involves operating security controls and services on an ongoing basis to maintain the security for the organization and to identify cyber incidents when they occur. This function may also include operating the organization's cyberdefense technologies, and overseeing the organization's incident response function (discussed in the next function).
- **Cyber Incident Response Team (CIRT)** involves responding to cybersecurity incidents and supervising their investigation and remediation. Frequently, this function is delivered from a team within the larger SOC organization.
- **Compliance** involves collecting artifacts that provide evidence that the organization's IT security controls and policies are operating as intended. The compliance team is responsible for "mapping" such artifacts to external compliance requirements and regulatory standards to demonstrate the organization's compliance with those requirements and standards.

Each of these functions requires specialized management, as well as technical and operational training tailored to the underlying operational processes and supporting IT systems. Security personnel require in-depth training that includes policies, procedures, and tools used for the organization's cyberdefenses. In addition, it is critical for security personnel to set examples of "good" security behavior by taking the required training; following organization policy, processes, and procedures; and helping to institutionalize the organization's security culture through their behaviors.

As an example of specialized cybersecurity training based on roles and responsibilities, security personnel who are CIRT members should receive training on: incident monitoring, forensic evidence collection, incident reporting, system recovery procedures, and cyber incident remediation. With such training, CIRT personnel will be able to interact with IT system users (particularly new users), and provide guidance to those users on the proper handling and reporting of user-perceived security incidents. Such peer-to-peer interaction can help system users understand the organization's day-to-day approach for handling cyber incidents. In this way, the organization can reinforce messages that help everyone protect organization information, organization devices, personal devices, and personal information every day.

Cyber Training for Partners

This training might be for partners, contractors, and other third parties. Partner training might include topics such as: custom software development, contract agreements, required security training, and contract compliance. Partners may be involved in many aspects of the organization's business, including providing software products, analysis services, onsite maintenance, or technology integration. Partners may also be a part of the organization's supply chain, contributing components of its products or services that are incorporated into the complete customer solution. For example, an organization may contract with a partner to develop custom software modules, along with appropriate documentation and training.

Partner training can take on many forms (e.g., web-based, self-led), and it should account for required organizational security processes, procedures, and controls. In some situations, the partner may work "off-site" at a location other than the organization's offices or factories. If the partner is working off-site, the organization should require the partner to design and develop its solutions in accordance with the organization's overall security architecture, including the implementation of organizational security controls. In addition, when manipulating the organization's data at the partner's location, the partner should provide comparable security protections to those used by the "on-site" organization, unless alternate protections are approved by the organization.

Agreements between an organization and partners can take many forms, such as contracts, licensing agreements, or joint ventures. The organization remains responsible for managing its risks, even though it may be using partners outside the organization. The organization needs to be responsible for assessing the risks of entering into partner agreements. Partner agreements should

include security requirements, roles, responsibilities, and required security training, along with the consequences for not complying with agreement terms and conditions.

Regardless of the types of agreements, an organization should require partners to comply with organizational security policies and procedures. Partner training should be designed to reinforce these messages, and spell out to partner management and personnel exactly what their obligations are regarding cybersecurity. For example, the partners should be required to notify the organization of personnel transfers or terminations so the organization can remove those individuals from lists of authorized system users. To help ensure compliance with security processes and procedures, the organization may continuously monitor partners' activities. Partners should consent to such logging and monitoring of their activities on the organization's IT systems. In addition, the organization should periodically review such activities with the partners. Such reviews may depend, in part, on the level of risk associated with the services, products, or personnel being provided by the partners.

Cyber Training for Specialists

This training might be for people in specialized roles not already discussed, or that emerge due to unique business requirements. Specialist training might include niche topics such as handling the internet of things (IoT), mobile technologies, or securing programmable logic arrays (PLAs). Specialists may be required for specific circumstances, such as introducing new technologies into an organization or providing specific expertise needed to accomplish organizational objectives.

For example, an organization may employ specialists who can provide consulting services regarding the internet of things (IoT). IoT consists of physical devices (e.g., mobile devices, computer hardware, biomedical devices, digital cameras, power grids) that collect and exchange data with each other over the internet. IoT technologies can be found in service sectors that include construction, energy, health care, life sciences, industrial, transportation, retail, public safety, and information technology. These items may be embedded with electronics, software, or sensors that can communicate with each other without human intervention. IoT specialists may provide professional consulting services on these technologies. Such services might include the following:

- Helping organizations plan, develop, integrate, design, and implement approaches for managing IoT instrumented and interconnected devices.
- Identifying and assessing IoT risks, along with suggested mitigation approaches.

- Providing IoT asset management and supply chain expertise.
- Recommending security approaches to help prevent, detect, and document attacks and compromises of IoT assets.
- Customizing IoT products to improve their security posture or address known vulnerabilities.

The goal of cyber specialist training is to identify such personnel, the security issues that may affect them, and appropriate training to address those issues. The organization should seek to provide specialists with appropriate role-based security training, in accordance with its security policy and procedures.

Chapter 12
Measuring Cyber Performance

How can organizations measure cyber success? How can organizations measure cyber failure, short of seeing their name in the news headlines or a call from the Federal Bureau of Investigation?

In business, performance is often measured in terms of revenue, profit, and expenses. In cybersecurity, performance can be measured in terms of risk and cost. While cost is easy enough to quantify, cyber risk is a lot trickier. Certainly, an organization can measure risk in terms of adverse consequences that actually occur, such as hacks or breaches. However, measuring such consequences is a little late in the game. It's preferable to measure cyber risk in terms of actions that might precede a hack or a breach, rather than after the damage is done. This anticipatory measurement approach is where security metrics can be useful.

Security metrics can enable organizations to quantify factors that relate to their risks. These factors indicate issues or activities that may precede or indicate an actual cyberattack. These factors may also indicate risk because they measure influences that contribute to the organization's vulnerability to potential cyberattacks. The idea is to identify metrics that can be objectively measured regularly without too much effort, and that help to create a picture of an organization's cybersecurity posture. These metrics help measure the assets, threats, vulnerabilities, and mitigations that make up the organization's risk management efforts.

Collecting organizational measurements related to cybersecurity is just the start. Once an organization collects those measurements, it needs to report, analyze, and track them over time. Some metrics will be required by regulations, standards, or outside auditors. Other metrics will be defined by organization employees or its leadership. Metrics may be measured with simple yes/no or pass/fail criteria, rather than numbers. There will be times when an organization is deficient, either by its own definition or when measured against external standards. There will be pressure to improve efficiency, reduce costs, and increase agility, all while maintaining desired cyber performance targets. Finally, there is the question of defining "good enough" cyber performance in an imperfect world and with imperfect tools for such measurement.

As shown in Figure 12.1, cyber performance measurement – consisting of security metrics, dashboards and reporting, audits and assessments, and deficiency, vulnerability, and risk tracking – supports and informs continual cyber improvement efforts.

https://doi.org/10.1515/9781501506529-012

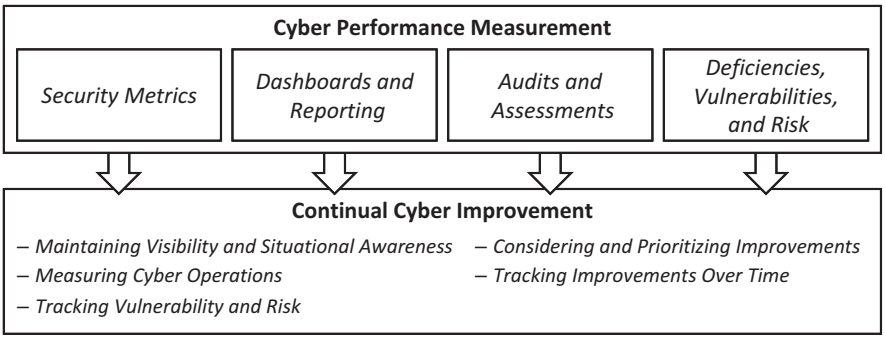


Figure 12.1: Cyber performance measurement helps an organization holistically visualize its cybersecurity program performance and supports cyber improvement investment decisions.

Simply stated, cyber performance measurement can help an organization understand its cyber posture, measure its cyber performance over time, comply with regulatory and external requirements, identify areas for improvement, define its cyber strategy, and navigate its cyber challenges.

This chapter starts with a description of a set of security metrics to help an organization understand its cyber risk. The chapter describes how to collect, present, and report these metrics using dashboards. Audits and assessments are then described in the context of helping management judge the organization's progress toward achieving its cybersecurity objectives and milestones. The chapter describes how an organization can track various types of cyberdefense deficiencies, and how it can track deficiency patterns back to business and cyber risks. Next, the chapter considers how organizational metrics can contribute to the continual improvement of its cybersecurity program. Finally, the chapter offers some insights into the organizational challenge of knowing when its cyberdefense is "good enough."

Security Metrics

The first step when establishing a metrics-driven security program is to define *what* to measure. While there is no single "textbook" approach to collecting security metrics, there are definitely some good practices that an organization can utilize. A major goal of an organizational cyber measurement program is to collect metrics that help tell the story of the organization's risk and its risk management efforts. An organization should collect metrics that describe its assets, threats, vulnerabilities, mitigations, and residual risks, such as the following:

- *Asset metrics* might track the numbers of users, computers, servers, applications, or sensitive records.
- *Threat metrics* might count scans, intrusion attempts, or track active cyber-attack groups.
- *Vulnerability metrics* might count identified vulnerabilities, missing patches, or compromised account passwords.
- *Mitigation metrics* might count security capabilities, security deployments, or track security upgrade projects.
- *Residual risk metrics* might track cyber incidents or known malicious activities.

When choosing an organization's metrics, it is helpful to pick numbers that can be easily tracked automatically and that can be monitored over time to detect trends and anomalies. Some metrics might be collected daily, while others might be collected monthly or even quarterly. Perfection is not the goal here – it is okay to add new metrics as needed and drop other metrics that are not yielding worthwhile information. An organization needs to be able to say, "Threats to our organization are up because 'ABC' metric is trending upward," or "We are more vulnerable because 'XYZ' metric is trending downward." Metrics deliver data to help visualize the organization's cyber posture and reinforce its cyber message to stakeholders that include employees, customers, partners, and auditors.

The remainder of this section describes some security metrics that can be collected and tracked by an organization's security team over time, as shown in Figure 12.2.

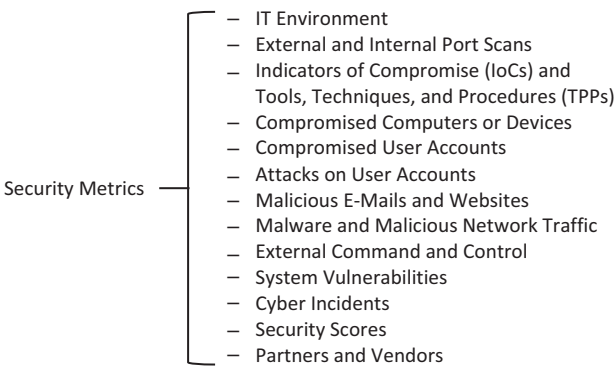


Figure 12.2: These representative metrics are usually relatively easy to collect and can help to illustrate an organization's cyber situation to management, employees, and other stakeholders.

IT Environment

Some of the first metrics to collect are those that describe the organization's IT environment. Such metrics include the numbers of employees, customers, computers, devices, facilities, servers, networks, and factory or medical devices. While these numbers are often steady-state (and don't need a lot of day-to-day attention), sudden changes to these numbers may correspond to significant cyber risks. Sudden growth, layoffs, or changes in technologies will often bring with them increases in cyber concerns. Also, activities such as reorganizations, relocations, mergers, acquisitions, or divestitures may also cause sudden changes to the organization's IT situation and cyber posture.

External and Internal Port Scans

One of the easier metrics to collect is firewall alerts detecting port scans against the organization's external or internal network interfaces. Port scans against external firewall interfaces are one of the less useful metrics to collect, as they can vary widely with little correlation to the risk of actual cyberattack. On the other hand, port scans against internal firewall interfaces are one of the better indications of malicious activity, particularly when those firewalls segment the network or protect critical internal IT infrastructure. Similarly, key servers may be able to detect when they are port scanned from a remote host, which can also be a strong indicator of a compromised internal system.

Indicators of Compromise (IOCs) and Tools, Techniques, and Procedures (TTPs)

Known attack patterns are often characterized as IOCs or TTPs. Some of these patterns may come through automated feeds from security providers or open source services. Other patterns may come from publicly available information or cybersecurity reports on specific attack methods. Certainly, the presence of IOCs or TTPs within the organization's IT environment is a strong indicator of active threats. Specific details about the IOCs and TTPs that the organization tracks may also be good indicators of a change in the threat environment. All of this information can be useful data to report.

Compromised Computers or Devices

An extremely important metric to track is occurrences of compromised computers or devices in the organization's IT environment. In IT environments where authorized users have access to the internet, can receive e-mail, or can take laptops or mobile devices home with them, user devices will be compromised on a somewhat regular basis. In these situations, the organization should be constantly detecting and remediating compromised devices, and carefully tracking these numbers to monitor the trends and reasons behind them. In addition, similar metrics should be tracked for servers, mobile devices, and network-connected equipment. By tracking these metrics, the organization can communicate the significance of the compromised device challenge and quantify the effectiveness of its response.

Compromised User Accounts

At the same time that the organization is tracking compromised computers, servers, and devices, it should also be tracking compromised user accounts. This tracking can apply to privileged administrator accounts, regular user accounts, guest accounts, and even customer accounts. It is helpful to track the number of compromised accounts, how those accounts were compromised (if known), and how the organization subsequently remediated the compromised accounts. For many accounts, remediation is as simple as changing a password, but sometimes it may be desirable to rename accounts, recreate accounts, or replace multifactor authentication tokens. When computers and devices are compromised, it may be prudent to consider all of the user accounts associated with those computers or devices to be compromised as well.

Attacks on User Accounts

While it is helpful to count known account compromises, it may also be helpful to track attempted attacks against accounts, even if such attacks do not succeed. Attacks against organization accounts may be strongly indicative of targeted cyberattacks. The most common way to track attempted attacks is to record log-ins and failed log-ins, and then perform analytics against them to detect attempts at account compromise. These analytics may also detect accounts that were already compromised without the knowledge of the account owners. This approach can be particularly helpful when there are additional

account protections in place – such as multifactor authentication (MFA) – that make it harder to exploit compromised account passwords.

Malicious E-Mails and Websites

Another useful predictor of overall cyber threats has to do with malicious e-mails and websites. Frequently, malicious e-mails can be caught by your e-mail provider, spam gateway, or e-mail anti-virus tools. Similarly, malicious websites can be caught by web gateways, network screens, and browser security tools. Since these tools are not 100% effective, some malicious e-mail and websites are going to get through them. By tracking how many malicious e-mails an organization receives, and how many malicious websites authorized users visit, an organization can gain visibility about how dangerous of its cyber environment is and how hard the security tools are working every day. By assuming that some number (say, 1%) of malicious e-mails and sites are going to get past, an organization can pretty accurately estimate how much actual danger is being passed on to its last line of defense: the users.

Malware and Malicious Network Traffic

Similar to how an organization can analyze e-mail and website traffic to understand how much danger is being passed on to users, it can also look at metrics from its internal security tools to track incidences of actual malicious software, as well as malicious or potentially malicious network traffic within the IT environment. These metrics can help track compromised devices, compromised applications, and signs of compromise that may require additional investigation. All of these metrics are strongly indicative of an organization's overall cyber risk.

External Command and Control

A specific type of malicious network traffic that warrants additional attention is command and control traffic. This network traffic originates from inside an organization's network environment – or its endpoints even if they are outside the network – and attempts to connect to attacker control servers over the

internet. Such traffic usually uses web browsing protocols HTTP and HTTPS[1] on the network ports 80 and 443, respectively. However, attacker command and control traffic may also be "tunneled" through virtual private networks (VPNs), through other protocols like file transfer protocol (FTP) or domain name system (DNS), and may even be conducted over e-mail. How well an organization can detect command and control traffic is going to partially depend on its network defenses. An organization should document such incidents and track them over time to help measure its network defense performance.

System Vulnerabilities

Another powerful but noisy set of metrics to track is system vulnerabilities collected from organizational vulnerability scanners. Just as a person's weight can vary from day to day, the numbers of vulnerabilities in an IT environment will likely vary widely as new vulnerabilities emerge and older vulnerabilities are patched or remediated. However, by tracking these results week after week and month after month, an organization can gain useful intelligence about its overall cyber posture and the diligence of its IT personnel in maintaining that posture. When tracking vulnerability metrics, organizations should analyze unpatched vulnerabilities in terms of severity and age. Severe vulnerabilities that remain unpatched for a long time can pose serious risk to an organization, particularly when those vulnerabilities are present on internet-facing or end-user systems.

Cyber Incidents

A discussion of cyber metrics would not be complete without discussing the biggest metric of all: cyber incidents. Cyber incident metrics may be captured within some of the other metrics an organization collects – including compromised accounts, computers, malware, and malicious network traffic – although incidents should also be their own metric category with their own analyses and commentary. Incident reporting should include analyses of the business impacts of the incidents, such as service outages, compromised accounts or records, costs of damages, or reputational harm. It should also include estimates of "close calls" where an incident did not actually occur, but the organization came close to suffering from an incident. By tracking these types of cyber

1 Hypertext transmission protocol (http); hypertext transmission protocol secure (https).

metrics over time, an organization can construct a detailed and informative story about the necessity and value of its cybersecurity investments.

Security Scores

Other useful metrics for an organization to consider are "security scores" that can provide insights into its cybersecurity posture. Assessors or internet-based security scoring services can help organizations manage cybersecurity readiness and comply with regulatory frameworks and standards. While internet-based security scoring scans provide information that is a secondary indicator of an organization's actual security posture, the scans may detect vulnerabilities, misconfigurations, or other security issues worthy of remediation. Internet-based scoring methodologies, while often proprietary, can provide a useful third-party "barometer" of an organization's security ecosystem that includes its partners and vendors. Certainly, when such metrics agree with other organizational metrics, they can reinforce positive or negative security messaging. When such metrics disagree with organizational metrics, the conflicting results may be a justification to do additional investigating to see if, perhaps, the organization is missing something important.

Partners and Vendors

Finally, an organization should keep an eye on its supply chain, including its technology partners, vendors, and customers. An organization should track how many partners, vendors, suppliers, and customers it has, and report on any available information indicating that they may have become compromised. In particular, large-scale breaches of internet user accounts may be cause for an organization to raise its security posture and protect against compromised user accounts, brute-force attacks, and incidences of password reuse. An organization should monitor information-sharing connections with its partners and vendors to reduce its attack surface through these connections, and to protect itself against potentially malicious activity originating from their end. An organization may also track security metrics related to partners and vendors, such as numbers of external accounts or connections, incidences of compromised accounts or connections, or other metrics that may be indicative of potential compromises.

Dashboards and Reporting

As an organization selects its security metrics to measure, a next step is to consider how it can collect, present, and report on these metrics over time. Some metrics may be easily presented through the interfaces of the applications collecting them, while other metrics may be most useful when correlated or cross-referenced with other data. Some metrics – like daily, weekly, or monthly counts – may be useful when presented in a static format. Other metrics like workloads or free capacity are best presented in real-time. Some metrics may only be useful if they are analyzed over time to identify trends, peaks, dips, or other fluctuations. Finally, there will be metrics that require fusion and analysis to identify patterns that may be of interest or may warrant further investigation.

These visualization methods are the "user interfaces" to organizational metrics, so it is important for such metrics be developed with the consumers in mind. Some visualizations may be better geared for technical staff, while others may be better geared for management. The goal is to find a balance so that everyone can get the data they need. The remainder of this section describes some visualization methods that can be used for presenting organization metrics, as shown in Figure 12.3.

Figure 12.3: Dashboards and reporting methods provide organizations with multiple ways to visualize their cybersecurity metrics, and then track metrics' performance over time.

Security Application Dashboards

Most mainstream enterprise security tools today have a "dashboard" view intended to present the viewer with the most important activity of the system – all on a single screen. From that screen, analysts can usually click once or twice to "drill down" into particular alerts or data elements. Vendors frequently design these default dashboards to demonstrate tool features to new customers and managers making purchase decisions. While often a good start at visualizing security data, these dashboards may not be really useful in day-to-day

practice. Therefore, an organization will likely need to customize the default dashboards to make them *really* useful, or will need to use other visualization tools to pull together the relevant data their analysts need.

Log System Dashboards

Due to their collection of data from a variety of sources and their flexible data handling capabilities, log systems may also be good sources of visualization. Log systems are frequently good at bringing together large numbers of logs onto common timelines, aligning log data into common taxonomies, and filtering log feeds for pre-identified alerts or noteworthy critical events. They may also be able to handle many types of data like dates, computer names, network addresses, or user identities buried in log entries. They tend to be weaker at performing charting or visualizations beyond basic capabilities.

Security Information and Event Management (SIEM) Dashboards

SIEM systems[2] tend to excel at dashboard visualization, and this capability is one of the major reasons for investing in SIEM technologies. Advanced filtering, correlation, and dashboard visualization features should be available, along with out-of-the-box configurations that are designed to suit a wide range of organizational needs. SIEMs should be able to deliver dashboard visualizations well-suited to the needs of operators, analysts, incident response, and management. Advanced products will even have such view sets already configured "out of the box" and ready for customers to start using immediately.

Analytics Dashboards

SIEMs, for all their visualization power, are still general-purpose products – their capabilities tend to be focused around lists of data and single-dimensional line, bar, or pie charts. If an organization uses advanced analytics tools in its cyberdefenses, SIEM tools may not be well-suited to displaying those tools' diagnostic status or outputs. For this reason, an organization will likely want to use the

2 SIEM is technology for collecting and matching cybersecurity events and alerts, and supports investigating and tracking cyber incidents arising from them.

dashboard features of its analytics tools. These dashboards may include advanced visualizations like multidimensional graphics, time-based trending, or map-based geo-location. Analytics dashboards may also be able to provide advanced alerting and correlation beyond the capabilities of general-purpose SIEM systems.

Custom Visualizations

Despite the power of general-purpose visualization tools, it may still be necessary to create custom visualizations, or use customized tools to deliver visualizations tailored to an organization's IT environment, business priorities, or operational situation. With custom visualizations, dashboards are only limited by imagination and the available data. Custom visualizations can also tie security data to other datasets such as network diagrams, facility maps, or office plans. This type of situational awareness can save a significant amount of time during cyber incidents, enabling faster and more accurate security responses while reducing the risk of mistakes or inadvertent collateral damage.

Trending and Snapshots

It can be helpful to be able to visualize organizational cyber activity over time. Time-based visualizations include trending and snapshots. Trending allows an organization to see how key metrics are changing over time, often using two- and three-dimensional charts and graphs. Snapshots can enable viewing of previous dashboard data, and may include a "rewind" function that can quickly scan through large volumes of alerts and metrics. Both trending and snapshots can be very helpful for detecting and investigating advanced attacker activities.

Periodic Reports

Metrics and data should be summarized in periodic reports for use by management and business leadership. Typically, reports might be produced at daily, weekly, monthly, quarterly, or annual intervals. Daily and weekly reports tend to be more focused on event activity, while monthly and quarterly reports tend to be more focused on resource and budget considerations, along with summaries of notable events.

The Operations Wall

For real-time organizational cyber operations, status information should be brought together and integrated into an "operations wall" that operations personnel can monitor for situational awareness. If cyber operations are centrally located in a specific facility, this wall might be an actual physical display or a set of displays that allow data sharing and analysis of cyber data from multiple sources. For virtual or geographically distributed cyber operations, this wall might be a series of web pages or online application displays. What is important is that these displays reflect the organization's cyber operations status, and should be the starting point for cyberdefense operational activities.

Audits and Assessments

Organizational audits and assessments can be valuable sources of cybersecurity status information. Audits involve evaluating cybersecurity against established standards with the objective of determining whether an organization complies with the standards or not. Assessments involve evaluating cybersecurity using an established framework with the objective of evaluating organizational cyber performance in the areas of the framework. Generally, the output of an audit is going to be a "pass" or "fail" determination, along with a list of deficiencies that may need to be remediated. On the other hand, the output of an assessment is going to be a series of subjective or numerical scores organized according to the categories and subcategories of the framework, along with observations and recommendations for areas of improvement. An organization does not usually "fail" an assessment, though it may do poorly. Similarly, an organization can pass an audit even though it has deficiencies and areas where cybersecurity should be improved. Because audits and assessments are generally performed by people outside of cyber operations and according to established frameworks, they can provide an objective perspective on an organization's cybersecurity status. This status can be important when it involves regulatory compliance or contract obligations.

Audits and assessments tend to connect with cybersecurity operations in two ways. First, there may be aspects of organizational compliance that can be calculated in real-time, giving a real-time view of compliance status as a part of operational dashboards or other monitoring. Second, organizational audits and assessments may identify areas of cyberdefense that need additional scrutiny or monitoring.

Audits and assessments generate their own data sets that should be tracked, monitored, and trended over time. These data sets can be particularly helpful

when the same frameworks are used multiple times, perhaps over subsequent years. Tracking audit and assessment data sets over time can enable an organization to see how its cybersecurity status is improving or struggling, and then use that information to guide management priorities. Finally, audits and assessments can help management to judge an organization's progress toward achieving its cybersecurity objectives and milestones.

The remainder of this section describes how audits and assessments can measure cyber performance and inform an organization's cyber program activities, as shown in Figure 12.4.

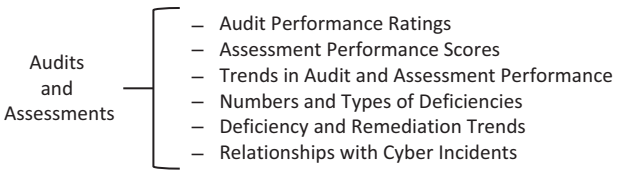


Figure 12.4: Audits and Assessments produce multiple types of data elements and metrics that can be useful inputs into the organization's overall cybersecurity measurement program.

Audit Performance Ratings

During an audit, organizational cybersecurity is often measured against objective standards, with the result being a "pass" or "fail" rating for each of the evaluated standards. Oftentimes, the overall rating may be based on aggregated data or analysis of large databases of data looking for deficiencies. An organization can track its overall performance against the evaluation criteria and the underlying data searches used for the overall performance rating. In cases where this analysis and tracking can be automated, it may be possible to monitor organizational audit performance status in real-time, which can be extremely useful as a detective control.

Assessment Performance Scores

During an assessment, organizational cybersecurity is often reviewed against industry-accepted frameworks[3] with the results based on the subjective judgement

3 One popular international framework was developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) – the ISO/IEC

of the assessor. Due to the subjectivity of assessment performance scores, they may not lend themselves well to automated checks or real-time monitoring. However, these assessment scores are often based on underlying data that is measurable and does lend itself to automated calculation. For example, if the assessor has a guideline that >70% is rated "good" and the "70%" can be automatically calculated, then an organization may be able to establish automatic monitoring of its assessment performance. This automation will most likely not be possible for the entire assessment score, but it may be possible for some of the assessment sub-scores that are of great concern or that have strong correlation with overall organizational cyber risk.

Trends in Audit and Assessment Performance

Importantly, once an organization has multiple audits and/or assessments against the same sets of standards or frameworks, it becomes possible to track trends in audit and/or assessment performance. Trending can be particularly helpful once an organization has data scores for three or more audits and/or assessments. Trending is challenged by the fact that standards and frameworks do evolve over time. Still, the results will usually be close enough year-to-year to provide decent visibility on how an organization is doing overall, and if its performance is improving or deteriorating over time.

Numbers and Types of Deficiencies

As an organization performs audits and assessments, the auditors and assessors will no doubt identify deficiencies and gaps in security controls that warrant attention. Tracking the numbers and types of deficiencies may provide useful strategic guidance about which parts of the organization's cyberdefenses may need additional attention. From an overall risk perspective, an organization will have to apply common sense when reviewing the types of identified deficiencies. For example, one deficiency in an organization's cloud configuration may be far more important than the two hundred internal user accounts with excess permissions.

27000 series of information security management standards. Other frameworks and standards for assessment are discussed in Chapter 5, "Cybersecurity Drivers."

Deficiency and Remediation Trends

Trends in organizational deficiency counts can be good general indicators on whether security is improving or deteriorating over time. Tracking remediation performance can also provide useful feedback, particularly looking at remediation performance over 30-day, 60-day, or 90-day periods. The following *representative* questions can help provide insight into an organization's trends:

- *Are deficiencies staying open for a long time or are they being resolved quickly?*
- *Are remediation efforts proceeding according to plan or are they being deferred in favor of more urgent operational needs?*
- *Are overall deficiency counts up or down as compared to last quarter or last year?*

By tracking and trending these numbers, an organization should be able to analyze this status and understand whether its performance trends over time are in line with its expectations and goals.

Relationships with Cyber Incidents

Finally, assessment scores and compliance posture may only loosely align with actual cybersecurity performance. As the old adage goes, "No combat-ready unit ever passed inspection." Similarly, just because an organization passed its last payment card industry data security standard (PCI DSS)[4] audit does not mean that its customers' credit card payment information is actually safe. PCI DSS audit results are just indicators and need to be treated as such. PCI DSS compliance issues should be treated as cyber risks – along with other known organizational cyber risks – and should be considered for remediation. Similarly, an organization needs to pay close attention to issues like vulnerabilities, malware, and attack indicators, which may be more indicative of potential cyberattack attempts. The greatest indicator of all is actual cyber incidents. Organizations that are suffering real cyber breaches should look critically at their cyberdefense posture, even if the results of their last assessment or audit were exemplary.

---

4 Organizations that handle credit cards from major credit card brands – such as Visa, MasterCard, American Express, and Discover – are required to comply with the payment card industry data security standard (PCI DSS) to help reduce credit card fraud.

Deficiencies, Vulnerabilities, and Risk

Cyber operational metrics can give an organization good visibility into its day-to-day cyber status, and audit and assessment results can provide visibility into its strategic cyber status. Dashboards and reports can help bring this data together into a comprehensive, multidimensional view of an organization's cyber situation. From that situational awareness, an organization should be able to identify its cyber deficiencies, vulnerabilities, and corresponding cybersecurity risk. By tracking and trending deficiencies, vulnerabilities, and overall risk, an organization will more easily gain useful insight into its cyber posture and the amount of difficulty attackers may have attempting to exploit it.

The remainder of this section describes ways an organization can track various types of deficiencies, vulnerabilities, and the cyber risk in its cyberdefenses, along with managing its mitigations and accepted risk levels, as shown in Figure 12.5.

Figure 12.5: Tracking deficiencies, vulnerabilities, and overall cyber risk provides an organization with visibility into its day-to-day and strategic cyber status. This status can then be used to inform its cyber metrics and risk measurement efforts.

Identifying Deficiencies to Track

Some of the most obvious deficiencies to track are those identified during a formal audit against an established cybersecurity standard. Audit deficiencies are also the ones with the clearest mandate for remediation. Less obvious deficiencies may be identified during cyber assessments, or pointed out by IT system operators. The challenge is that an organization can always find ways to improve itself, but it may not make sense to identify *everything* cyber-related that is "less than perfect." The organization should look at its critical IT systems and cyber systems and consider where the issues and challenges lie. From those issues and challenges, the organization may be able to identify patterns of deficiencies that can be addressed through modest investments or simple enhancements. Relatively simple cyber improvements, such as protecting highly

privileged accounts, may be able to mitigate entire classes of security deficiencies and cyber vulnerabilities.

Tracking Vulnerabilities

Software and operating system vulnerabilities are generally identified by vulnerability scanners that are run against the organization's network, but such vulnerabilities may also come up during red team tests[5] or cyberdefenses assessments. Vulnerabilities – particularly those that can be remediated by installing patches – can be distracting due to their volume and immediacy. To remediate patchable vulnerabilities, some people may think that all an organization has to do is install the patch! However, this situation can exacerbate a fundamental tension between cyber professionals who want to address security issues, versus IT professionals who need to maintain stable operational IT systems, with a minimum of downtime. While it is desirable to patch and remediate the vulnerabilities as they are found, that approach may not always be possible or practical. The challenge is that installing patches has impacts on IT operations, IT systems configuration controls, and can affect the stability of complex, multi-server IT applications. IT systems involving dozens or even hundreds of servers cannot be changed without planning. Organizations need to start by simply identifying and tracking these vulnerabilities so that they can be remediated at appropriate times, in conjunction with other IT operational requirements.

Tracking Cyber Incidents

Similar to deficiencies and vulnerabilities, organizational metrics and dashboards should give good visibility into cyber incidents against the organization. The goal here is to identify events and alerts that actually indicate deliberate

5 Red team testing can complement vulnerability scanning and vulnerability management by looking at vulnerabilities not only in terms of individual systems, but in terms of an entire organization IT system as a whole. A red team tries to exploit enough vulnerabilities or other security issues to successfully penetrate the organization's perimeter, establish a foothold inside the network, perform command-and-control, and them move laterally and escalate privileges to get to their target. If the red team is successful at penetrating the organization's cyberdefenses, then it will likely recommend additional security improvements to address the gaps that were exploited.

attacks against accounts, devices, or networks. These attacks might be evidenced by attempted abuse of accounts, malware or malicious behavior on devices, or suspicious network traffic. Metrics tracking cyber incidents may be divided into groupings to indicate *actual* attacks, attempted but *unsuccessful* or *incomplete* attacks, and *potential* attacks (i.e., not sure if detected activities were actual attacks). Metrics that indicate actual cyberattacks, whether those attacks succeed or fail, are some of the most powerful indicators of an organization's actual cyber risk.

Tracking Cyber Risk

Synthesizing together information about deficiencies, vulnerabilities, and incidents, the organization should be able to construct a comprehensive picture of its cyber risk. Risk lies at the intersections of assets, threats, and vulnerabilities. So, the organization will also have to track its assets and threats – along with its cyber deficiencies, vulnerabilities, and incidents – to build a complete risk picture. A key distinction here is that risk requires a business consequence – the confidentiality, integrity, or availability of an IT asset must be in jeopardy – for the risk to be worth considering. Otherwise, it is just a vulnerability. Also, an organization should not have too many risks, maybe ten to 100. Only the largest global organizations are going to be able to track more than a thousand risks. To keep risks manageable, the organization should group its risks together around the affected IT assets and threat vectors. Then the organization can consider which deficiencies, vulnerabilities, and incidents are tied to which cyber risks. With this understanding, the organization can perform its risk assessment, prioritization, and mitigation efforts. Note that a single vulnerability in a critical system like an internet-facing server or remote access device can have a significant impact on the organization's cyber risk posture, on very short notice. When critical vulnerabilities arise, the organization needs to be able to map those vulnerabilities against their cyber risks to understand the potential business impacts of the vulnerabilities, and then track the corresponding risks until the vulnerability can be remediated.

Managing Mitigations

When risks are identified and prioritized, the organization can take action to smartly manage its risk mitigation efforts. Mitigations may be as simple as patching known vulnerabilities, or they may be as complex as re-engineering

or upgrading IT systems to address unpatchable deficiencies.[6] Mitigations may reduce the *likelihood* of a risk being manifested or the *impact* of it occurring, but a single mitigation seldom reduces both the likelihood and impact together. On the other hand, a single mitigation may simultaneously mitigate vulnerabilities affecting multiple cyber risks. As the organization tracks its mitigations and the vulnerabilities they address over time, it can show which risks are being addressed, and to what degree.

Tracking Accepted Risk

After applying mitigations to risks, the organization will be left with a mitigated risk register that shows the posture of the organization's risks after the in-place and planned mitigation efforts are considered. This risk register can then be used to drive conversations with management about which risks should be accepted and which should not. Accepted risks may be accepted as a matter of course or may be mitigated through non-cyber processes like insurance or redundancy. Other risks may warrant additional mitigation over time to further reduce the risks or transfer them to third parties.[7] By tracking its risk posture over time, the organization can demonstrate how cyberdefenses efforts are affecting its risk posture, and how that posture may be trending upward or downward.

Continual Cyber Improvement

Cyber performance measurement can support the organization's strategic objective of improving its cyberdefense posture through continual cyber improvement. With good metrics and measurements in place, improvements should have visible impacts on the dashboards, visualizations, and other status information seen by cyber defenders and management. As the organization's cybersecurity program improves, it should see fewer warnings, perform

6 When software is at its end-of-support life, the vendor will no longer create patches for known vulnerabilities – the software is "unpatchable." Examples of unpatchable software include Microsoft's Windows XP and Windows Vista operating systems. Unpatchable software risks increase over time as attackers deploy new exploits to known vulnerabilities, and old vulnerabilities remain unpatched.

7 See Chapter 3, "Cyber Risk Management," for a detailed discussion of risk treatment approaches.

fewer investigations, and (hopefully) incur fewer incidents. As the organization's compliance posture improves, it should see fewer vulnerabilities, auditors should find fewer deficiencies, and cyber defenders should have to perform fewer remediations, at least in theory.

In practice, improving the cybersecurity program is seldom a simple activity. Sometimes, as visibility into cyberdefenses and detective controls improve, the organization will end up seeing *more* events and alerts that require investigation. Then, as the organization improves its filtering and fidelity to reduce false positives, it will see those numbers decline again. As its cyberdefenses improve, the organization may find that its auditors and/or assessors raise the bar for evaluation, resulting in yet more deficiencies to address. Hopefully, these deficiencies will be of lesser importance in terms of the risks they represent. As this data is reported to management, considerable interpretation may be required to convey the full nuance of the organization's actual cybersecurity status, and to help business leaders understand the data within its full business context.

The remainder of this section describes ways that metrics and measurements can contribute to the continual improvement of an organization's cybersecurity program, as shown in Figure 12.6.

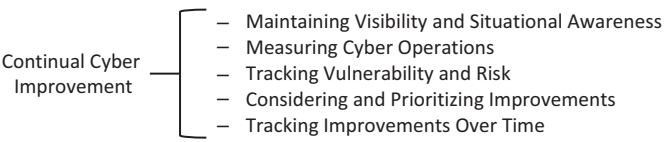


Figure 12.6: Continual cyber improvement can be informed by cyber measurements, which can also be used to measure the performance of cyber improvements as they are implemented.

Maintaining Visibility and Situational Awareness

One of the necessary elements to achieve continual improvement is visibility and situational awareness of the organization's cyber environment at any given moment in time. The organization can ask the following *representative* questions to help gain insight into its cyberdefense posture:

- *Are our preventive controls working?*
- *Are our detective controls are working?*
- *Are we in compliance with our regulatory or contractual obligations?*
- *Can we detect cyber incidents that require investigation?*

- *Can we look inside our IT environment to investigate device, network, and account activity that is of concern?*
- *While our cyberdefenses are operating, can management see what is going on in aggregate to be able to understand the big picture?*

This set of questions is not meant to be exhaustive. An organization should determine its own set of questions specific to its cyber environment and organizational needs. Answers to these questions, along with other relevant information, can help the organization gain visibility and situational awareness into its cyberdefenses and their operational effectiveness.

Measuring Cyber Operations

Once an organization has situational awareness, it needs to monitor its ongoing cyber operations. In addition to cyber professionals having situational awareness to identify and investigate events of interest, cyber managers should have an awareness of cyber operations activity. Managers need cyber operations to give them answers to the following *representative* questions:

- *How many investigations are taking place?*
- *What types of events are being investigated?*
- *What are the outcomes of those investigations?*
- *What defects, deficiencies, or vulnerabilities are those investigations revealing?*
- *What remediation is taking place to address those defects, deficiencies, or vulnerabilities after they are identified?*

By tracking and measuring cyber operations, cyber managers can understand how the organization's cyberdefenses are performing (or not performing), and where its cyberdefense operational challenges reside.

Tracking Vulnerability and Risk

With visibility into cyber situational awareness and cyber operations, an organization can build upon that combined visibility by considering its vulnerabilities (both patchable and unpatchable) and its overall cyber risk. Even though vulnerabilities may not directly link to cyber risk, newly revealed vulnerabilities can result in dramatic and immediate changes to an organization's cyber risk posture. This situation is particularly true if the vulnerabilities are not mitigated by compensating preventive, detective, or response cyber controls. By tracking both

vulnerabilities and cyber risks, an organization can achieve visibility of where its software systems may be vulnerable to attack, and the business consequences of those attacks manifesting themselves.

Considering and Prioritizing Improvements

With visibility into the organization's situation, cyber operations, vulnerabilities, and risks, the organization should be able to consider, evaluate, estimate, and prioritize potential improvements to its cyberdefenses. Cyberdefense challenges can help an organization decide where to make needed investments. For example, consider the following questions:

- *Are challenges related to cloud services, applications, endpoints, servers, accounts, or infrastructure?*
- *Is the organization seeing close calls on a regular basis with e-mail-delivered malware or executive fraud?*
- *Is the organization seeing regular penetration of its external cyberdefense perimeter, only to avert disaster through blind luck or cyberdefense heroics?*

Answers to these questions can be helpful to decision makers when they consider which cyber improvements will make the most impact, which improvements to do first, and the potential impact of improvements on the organization's overall cyber risk posture. With operational data to support investment analyses, it should be easier to make the hard decisions on cyber initiatives, and to justify those decisions to organizational management, staff, and partners.

Tracking Improvements Over Time

Once the organization has data-driven visibility into its cyber improvement roadmap and strategy, it can track that performance over time. While it may not make sense to monitor cyber enhancements on a daily basis, it probably does make sense to track cyber improvements on a monthly, quarterly, or annual basis. Generally, there are three aspects of cyber improvement efforts that should be tracked:

- How cyber improvements are reducing the organization's vulnerability to cyberattack.
- How cyber improvements are improving cyber operations, either by reducing incidents or by making incidents easier to investigate or remediate.
- How cyber improvements are reducing organizational risk.

By tracking improvements over time, the organization can understand and share with others the business value that cyber is delivering. Most importantly, the organization can tell the cyberdefense story in terms of the business risks that are of greatest concern to leadership, and how those risks are being mitigated.

Knowing When to Stop

At the end of the day, one of the greatest cybersecurity challenges is deciding when and where to stop.

What is "good enough" cyber performance?

On the one hand, few cyber professionals are going to admit that their cyberdefense is actually good enough. On the other hand, the reality is that resources are limited, priorities must be established, and cyber is only one of a great many business risks that the organization must consider. Sometimes, cyber can best serve the organization by saying it is "good" and that resources can be better used elsewhere to help address other risks, rather than investing in more cybersecurity. The following two types of metrics can help the organization identify when it has achieved "good enough" cybersecurity performance:

- ***Visibility and Monitoring Metrics.*** These metrics provide an organization with insight into actual cyberattacks against the organization. If the organization does not have this insight, it cannot judge if it is being attacked or not, nor can it judge if the cyberdefenses are working against the attacks that are occurring. If the organization has this visibility, and the metrics indicate that it is not being attacked successfully, then this data could be an indicator that the organization's cyberdefenses are serving their purpose and be adequate to the task.
- ***"Success" Metrics.*** These metrics involve defining "success" in terms of the cyber information that the organization has available. Perhaps a success metric might be "one compromised account per month," or maybe "no signs of cyberattack on internal IT networks in the past 90 days." Key to defining success metrics is first having visibility and monitoring metrics. An organization cannot have confidence that attacks are not succeeding if it does not have monitoring to detect such attacks when they occur.

The challenge here is to try to prove a negative regarding cyberdefense performance. An organization cannot have confidence in what it is *not* seeing, if it

doesn't first have confidence in the visibility and monitoring delivered by its metrics and dashboards.

But how does the organization economize on cybersecurity? It probably would not be prudent to suddenly turn off the firewalls or uninstall the antivirus software. However, these are only two parts of what is often a highly complex cybersecurity environment with many hardware and software components sourced from a multitude of vendors. Consider the following *representative* questions regarding evolving an organization's cybersecurity posture:

- *Can the organization replace a branded product with an open source package, and reduce licensing and support costs?*
- *Can the organization replace two "best-in-class" products with one "general purpose" product without losing significant cyberdefense capability?*
- *Can the organization reduce its licensing costs by reducing the amount of monitoring it is doing or vendor product capacity it is using?*

The answers to these questions may drive changes to the organization's cyberdefense technology platforms. While reducing costs, these changes may also reduce the effectiveness of the organization's cyberdefenses. Impacts to the organization's cyberdefense effectiveness may include the following:

- Changes that reduce the organization's cyberattack prevention abilities may allow more attacks through, but should not impair the organization's ability to detect, respond, and recover to the attacks that occur.
- Changes that reduce the organization's cyberattack detection may impair the organization's ability to catch cyberattackers; as a consequence, they should be handled carefully.
- Changes that reduce the organization's cyberattack recovery ability may be okay if attacks are not succeeding and recovery is not usually necessary.
- Changes that reduce the organization's cybersecurity system complexity can be the most beneficial, since they can reduce ongoing maintenance costs as well as product licensing costs.

Simply stated, when an organization is economizing on cybersecurity, it needs to systematically think through the preventive, detective, response, and recovery impacts of the proposed changes. The remainder of this section describes how organizations can use their cybersecurity metrics to inform efforts to manage cyberdefense spending and potentially free up resources to support other business priorities, as shown in Figure 12.7.

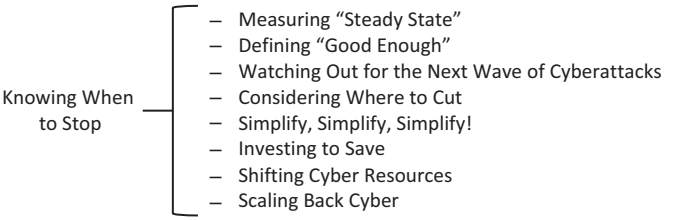


Figure 12.7: An organization can use its metrics, measurements, and visibility to evaluate its overall cyberdefense posture and decide where to adjust and economize on its cyberdefenses.

Measuring "Steady State"

One of the first steps in knowing what is "good enough" cyber performance is being able to measure the "steady state" of cyber operations. An organization needs to be able to see the cyber activity within its environment. When it can see the cyber activity, the organization can have confidence that it is not taking unacceptable risks when it reduces its cyber capabilities. When measuring its cyber performance, an organization will want to measure its cyber steady state over relatively long-term windows – such as months or quarters. Of course, measuring cyberdefense steady state can be made significantly more challenging by IT environments that are constantly changing and seldom in a "steady state" of their own.

Defining "Good Enough"

The second step in economizing on cybersecurity is to define organizational metrics and measurements within its IT environment for measuring that the operating cyberdefenses are performing adequately against their business requirements. Things are usually good enough when cyberattack activity stays below certain thresholds over a period of time, based upon good visibility on the cyber activity within the environment. This visibility should include cyber activity relating to computers, devices, networks, and user accounts. The period of time for this visibility should not be too short – at least one or more quarters – so the organization can have confidence that its cyberdefenses really are performing well enough.

Reducing cyber capabilities is a strategic decision that should be based on strategic measures,and then carefully monitored to make sure it is achieving the desired business goals.

Watching Out for the Next Wave of Cyberattacks

When considering visibility and cyberdefense adequacy, watch out for waves of cyber activity. Sometimes, there may be a surge in cyber activity – that is, a wave – in conjunction with new vulnerabilities, new exploits, new malware, or new attack techniques. During these times, an organization may see sharp increases in cyberattacks or cyberattack successes, which can result in a significant increase in the organization's cyber risk. When reducing cyber capabilities, remember that the next wave may be right around the corner. Have sufficient extra capacity in the organization's cyberdefenses to be able to handle that next wave of cyberattacks when it occurs.

Considering Where to Cut

As the organization looks at ways to economize its cyberdefenses, a particular challenge is identifying where cyber spending can be reduced. Opportunities to reduce cyberdefenses may include the following:

- *Cyberdefense capabilities* that are seldom used, are redundant, or can be consolidated with other cyberdefense capabilities using a single technology.
- *Overlapping* preventive, detective, or recovery controls, where one or more controls can be reduced, consolidated, or eliminated.
- *Reducing the scope* of cyber controls so that less of the IT environment is being protected, monitored, or recovered, reducing cyberdefense licensing and maintenance costs.
- *Accepting additional operational cyber risk* in areas of the business, in exchange for reduced cybersecurity costs.

By exploring these opportunities, the organization may be able to identify areas where cyberdefenses can be reduced, with a limited impact on the organization's actual business risk.

Simplify, Simplify, Simplify!

In general, the best value for reducing cyber costs is by simplifying the organization's cyberdefense and IT environments. The following areas may be opportunities for simplification:

- *Identifying cheaper alternatives* where a cybersecurity product is deployed to serve a small scope or a narrow niche within the cyberdefense environment.

Can the product be replaced with a cheaper alternative, or can it be eliminated altogether?

- *Identifying areas* where there are multiple technologies delivering similar or overlapping capabilities. *Can those functions be consolidated into a single technology?*
- *Re-considering "Best-in-class" technologies* that may be more capable than what is actually needed. *Can those technologies be replaced with open source or suite alternatives that work almost as well?*
- *Re-engineering the cyber architecture* and how it aligns with the organization's IT environment. *Can IT re-engineer the IT environment so it is simpler and easier to secure?*

With cyber environments that have been evolving for a long time, there tend to be tremendous opportunities to simplify the environments and remove complexity. When this is done, the organization can enjoy lower costs and fewer maintenance headaches going forward.

Investing to Save

Cyber change is not free. One of the biggest challenges in reducing cyberdefenses and simplifying cyber architectures is the cost of the investment required to actually make the change. This investment should be looked at in terms of simple return on investment (ROI). The goal with these types of changes is an ROI of fewer than three years. With many IT technologies on a five-year lifecycle, an organization may be able to synchronize its planned changes with other necessary technology retirements, and achieve a rapid ROI for changes synchronized with IT technology lifecycles.

The organizational challenge here is making the necessary investment at the right time and in the right places. It may be necessary to re-engineer certain cyber technologies to simplify their architectures or technologies, without compromising their capabilities. Such re-engineering efforts may require more advanced skills than the skillsets of the available cyber operations personnel presently operating the organization's cyber technologies. Organizations that operate according to the IT Infrastructure Library (ITIL)[8] will often have a strict separation of IT operations from engineering. These organizations may not have the skills in-house to re-engineer operational cybersecurity. Depending upon the required re-engineering, the organization may need to engage outside consultants

---

8 Information Technology Infrastructure Library (ITIL) is a set of IT service management (ITSM) practices designed to help align IT services with business needs.

or vendor professional services to get the expertise it needs to make the required changes. Cyber leadership will need to work with business leadership to estimate the level of effort involved and the skills required to do the work. Once the organization has those estimates, the cyber team can work with business leadership to make the appropriate investments, and then oversee the execution of those investments to achieve the desired cybersecurity objectives.

Shifting Cyber Resources

As an organization makes investments in cyber changes and cyber re-engineering, it should find itself freeing up operational resources that can be given back to the business or shifted toward other priorities. Adopting a "DevOps" model[9] for cyber technologies, where development and operations are closely linked, may improve cyber agility – although this model may also run counter to established ITIL methodologies. When making these shifts, an organization may also find that the shifts have impacts on personnel and staffing model. Employees who are operating or engineering technologies that are going away may have less to do. Technologies that are becoming more complex may generate more work than the available employees can actually perform. The point to be stressed here is that the organization needs to take care of its talented cyber professionals. It is often easier and cheaper to invest in training for the existing employees than to try to hire new employees with the necessary skills, and then train them on the nuances of the organization's IT environment. Consultants may be able to help make the changes needed, and then cross-train the existing employees to maintain daily operations going forward. Key here is keeping track of the organization's cyber spending, reducing that spending in areas that need less attention, and then using those savings to invest in the areas where additional cyber capabilities are needed.

Scaling Back Cyber

When determining what is "good enough," the general business objective is to scale back cyber capabilities so that they are as small and as cheap as possible while still accomplishing the desired business risk mitigation objectives.

9 DevOps is a software engineering practice designed to integrate development (i.e., software developers) and operations (i.e., IT infrastructure professionals) teams to achieve rapid development cycles that frequently and reliably deliver software products, features, and services to customers.

Organizations should remember that cybersecurity often gets in the way of the types of agile IT operations that the organization needs to transform itself to address future business challenges. When cyber risk is being adequately but not excessively handled, the organization may not feel like its cyberdefenses are comfortably covering all of the possible cyberattack scenarios. If cyberdefenses feel like they are comfortable, the organization may be over-investing in cyber capabilities and missing an opportunity to cut back. Cyber is only one of many business risks, and should not be handled "better" than the other risks that can also jeopardize the organization's business and revenue.

International competition, personnel recruiting, proprietary technologies, and manufacturing processes are all sources of risk to the business. While cyber can help address many of these business risks, other factors such as cost control, solid accounting, and business strategy should also be considered. By reducing its cyber spending and scope, the organization expands options for the rest of its business, and may help its overall risk management effort stay balanced among cyber, industrial, business, regulatory, and competitive risks. All of these risks exist side-by-side, and they must all be considered, equally.

Chapter 13
When Things Go Wrong

So far, this book's chapters have focused on the great things an organization can and should be doing to have effective cybersecurity. The book has not focused on the countless things related to cyber that can and will go wrong.

Remember Murphy's Law? "Anything that can go wrong will go wrong."[1]

If an organization's cyberdefenses rely upon every component working "perfectly" all of the time, and all the employees doing their parts "perfectly" all of the time, it is likely that cyberdefense success will be lacking – most likely on a regular basis.

The reality is that IT and cyber are complex endeavors using complex technologies where perfection is not only elusive but is also most likely impossible to achieve. Ideally, the goal is that even when some cyberdefenses fail or are defeated, an organization will continue to be protected. This protection might come from resilient cyberdefenses that include backup preventive controls, detection and response controls, and rapid recovery controls.

This chapter is not about what happens when the primary defense fails and the backup defense works. This chapter is about what happens when the attackers succeed and the organization finds itself in a difficult and uncomfortable situation.

- Perhaps the organization got a call from the U.S. Federal Bureau of Investigation (FBI), or another law enforcement agency.
- Perhaps its customers reported fraudulent credit card transactions, or its banks reported issues with the organization's banking accounts.
- Perhaps ransomware took out most (if not all) of the organization's computers or disabled its manufacturing facility.
- Perhaps employees came into work one day to find the power out or the factory machines inoperative.
- Perhaps the organization's most sensitive internal correspondence got posted to a public website.

---

1 Spark, Nick T. *A History of Murphy's Law*, Periscope Film, ISBN-13: 9780978638894, May 21, 2006.

https://doi.org/10.1515/9781501506529-013

All of these events have actually occurred to unsuspecting organizations whose cyberdefenses were defeated, within recent history. These events are cyberattack realities that affect the confidentiality, integrity, or availability of organizational IT systems and assets. These three main types of cyberattacks against organizations have the following characteristics:

- *Confidentiality* attacks result in breaches of sensitive, protected, or regulated data.
- *Integrity* attacks result in unauthorized changes to sensitive information or records.
- *Availability* attacks result in outages that disable organization computers, devices, accounts, or networks.

When these attacks occur, an organization must be prepared to quickly move into "crisis mode" and deal with the consequences of coming face-to-face with a skilled adversary who means to do harm. This chapter describes what happens *when things go wrong* with cyberdefenses and what organizations can do to counter the cyberattackers and protect the organization. Figure 13.1 shows *representative* incident management activities and long-term cyber protections that organizations can implement to deal with the damage that can be caused by modern cyberattacks.

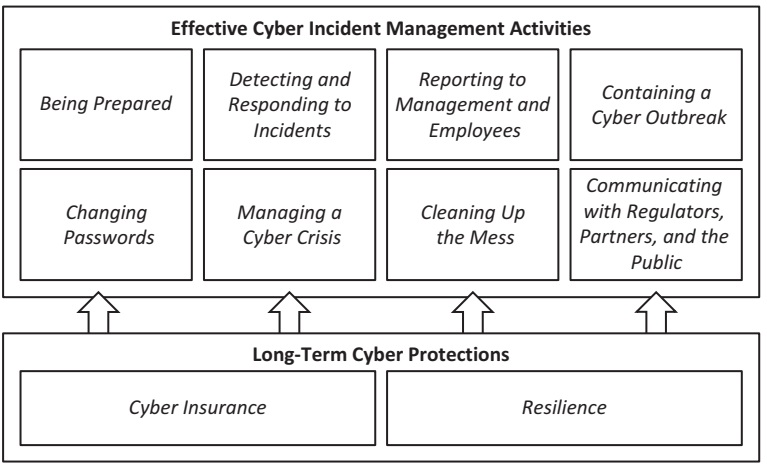


Figure 13.1: Serious cyber incidents follow a particular process, whereby the organization detects, analyzes, responds to, and recovers from the actions of the attacker; insurance and resilience can greatly reduce the costs and pain of responding to serious incidents.

Being Prepared

Effective cyber incident management starts with being prepared and thinking through the possibilities of what could go wrong, and what an organization can do "now" in anticipation of those possibilities. Technologies are going to fail, people are going to make mistakes, and plans are going to go awry. Murphy's Law is alive and well. Today's increasingly complex IT systems make it easy for things to go horribly wrong, especially in the face of a determined adversary.

To prepare for possible cyber incidents, an organization needs to account for the following major incident response elements:

- *People* with important roles in an incident need to be identified, be advised of the roles they might play, and be involved in the planning and preparation processes.
- *Plans* should be prepared by thinking through various cyber incident scenarios. While the plans do not have to be overly detailed, they need to reflect some level of thinking about what might go wrong and who would need to do what to address the situation.
- *Resources* need to be identified and should include those resources: (1) needed to support the planning and preparation process; (2) needed to execute the various contingency plans; and, (3) that can be quickly arranged in the middle of a difficult situation.

This section considers some of the topics an organization should consider when preparing for cyber incidents and potentially serious cyberattacks. These topics are shown in Figure 13.2.

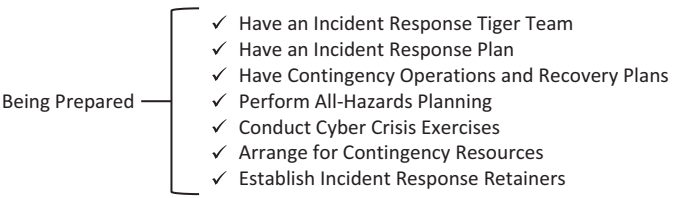


Figure 13.2: Being prepared includes identifying the people, plans, and resources that might be helpful to address a wide range of potential cyber incident scenarios.

Have an Incident Response Tiger Team

Perhaps the most important step in cyber incident preparation is identifying the people who might be involved, and sharing with them what might happen

and what their roles might be in the case of a cyber incident or situation. This step involves not only cyber and IT personnel, but also cross-functional roles like business leadership, human resources (HR), legal, compliance, communications, public affairs, and law enforcement liaisons. In complex organizations with multiple business units, it might be necessary to coordinate across corporate lines or to interface with home offices. In services organizations, it may be necessary to include contract managers and customer relationship executives.

An organization will find that plans to respond to different types of cyber situations involve different groups of people. One Tiger Team approach is to have a core team that is involved in almost every incident, and secondary teams that are only activated if they are needed – depending on the situation and the stage of the incident. By having this tiered-team structure, everyone knows their role, but secondary personnel are only brought in for situations that involve them. In this way, the time of secondary personnel is not wasted on situations that do not involve them.

Have an Incident Response Plan

Once the team is identified, the next step is to establish the core incident response plan. This plan can be as detailed as needed, but should include the following basic information:

- Criteria for declaring a cyber incident
- Personnel to be notified in response to an incident
- Meeting attendance and formats for incident coordination
- Basic reporting structure for disseminating incident information
- Process for scoping the incident, and identifying required personnel and resources
- Procedures for activating incident response resources
- Process for escalating or re-scoping the incident, if necessary
- Process for managing business impacts related to the incident
- Process for handling coordination and communication with internal, external, and law enforcement stakeholders
- Process for resolving the incident
- Closing vulnerabilities and strengthening defenses
- After-action reports and reviews

Incident response plans should include thinking through how to sustain operations during the incident, while repelling cyberintruders in such a way that it will be hard for them to get back into the organization.

Have Contingency Operations and Recovery Plans

In the event of a serious incident, it may become necessary to isolate, disable, reset, or rebuild parts of an organization's IT infrastructure. This situation can include accounts, networks, computers, servers, or devices involved in delivering an organization's business. In manufacturing or healthcare, affected systems may include those necessary to keep the plant running or to care for patients.

Contingency operations and recovery plans consider how an organization might be able to keep operations going under these circumstances. This might include the organization operating with its IT systems impaired or even completely unavailable. For example, an organization might consider the following questions:

- *Are paper records and paper-based processes available?*
- *Can plant equipment be operated while disconnected from the network or while the network is unavailable?*

An organization also should plan out the steps that might be necessary to restore IT operations after the incident. These steps might include resetting accounts and passwords, replacing endpoints and mobile devices, rebuilding servers and applications, and re-configuring networks. These plans may include the use of alternative resources like backup data centers, cloud services, and backup data sources. The plans should also consider recovery point objectives (RPO) and recovery time objectives (RTO)[2] for restoring business applications and data.

Perform All-Hazards Planning

As an organization considers cyber incident possibilities, it will want to consider that cyber is not the only source of potentially significant IT or operational outages. Natural disasters, accidents, mistakes, and criminal activity can also have devastating effects on an organization. In fact, the IT impact may be the least of an organization's concerns, especially if its people are in peril, its equipment is disabled, or its facilities are damaged.

---

2 Recovery point objective (RPO) is the point in time that data is recovered through. For example, if the recovery point is nightly, then a recovery will not include transactions from the following day. Recovery point is about how up-to-date data needs to be. Recovery time objective (RTO) is how long it takes from when the disaster is declared until the system can be recovered and its data and transaction processing capabilities are available again. Services will be unavailable until the recovery can be completed, so a long recovery time can be difficult for operations.

Many organizations have found that the organizational responses to these different types of hazards need to involve the same people, processes, and approaches. All-hazards planning accounts for these factors by considering cyber as only one of many possible hazards jeopardizing an organization, and that all hazards have commonalities. All-hazards planning organizes cross-functional responses that are consistent for the entire organization, while also being flexible to handle a wide range of possible crisis scenarios. This approach is particularly helpful for large organizations, since it establishes one simple, standard process that everyone knows will be followed regardless of the specifics of the crisis situation. Once the incident response has been initiated, the organization can then tailor its activities to include the right people, plans, and approaches.

Conduct Cyber Crisis Exercises

Perhaps the best way to figure out what an organization needs to do in a cyber incident or crisis is to conduct exercises. Exercises may range from a couple of people brainstorming on a whiteboard, to tabletop scenarios involving incident response teams, to full-blown simulations involving outside consultants and event facilitators. Exercises should focus on the following *representative* aspects for preparing for when things go wrong:

- *Who are the people?*
- *What is the plan?*
- *What resources will be required?*

Exercises should also consider the following representative time frame questions:

- *How long does it take to initiate the incident response?*
- *How long will it take to notify people?*
- *What is the tempo for coordination within the incident response?*
- *How long will it take to make decisions?*
- *How long will it take to arrange resources?*
- *Are these time frames adequate for the organization to adequately respond to rapidly changing crisis situations?*

Cybersecurity incident exercises should be built around realistic scenarios such as malware, compromised accounts, ransomware, internet failure, data center malfunction, or cloud service outage.

Arrange for Contingency Resources

In considering response time frames for a crisis situation, an organization may discover that, in many cases, the standard response process is not going to be fast enough to meet its needs. For example, the middle of an incident is a poor time to negotiate contracts, buy new equipment, configure software applications, or stand up cloud services. In such cases, it is prudent to arrange contingency resources ahead of time.

While contingency resources may not be free, they will likely be much cheaper than trying to make emergency arrangements in the midst of a crisis situation. Also, by arranging for contingency resources when an organization is unhurried, it can conduct appropriate due diligence, consider alternatives, and negotiate to get a reasonably good deal. Having contingency resources already arranged is critical to recovering when minutes count and when outages are costing thousands or even millions of dollars per hour.

Establish Incident Response Retainers

An important part of contingency resource planning is arranging for skilled and talented people who can augment core personnel in the event of an incident or crisis. An "incident response retainer" arranges for such people to be available and "standing by" should something occur.

While most often used for cybersecurity forensics and investigation personnel, incident response retainers can also be used to have systems administrators, software developers, or other IT professionals be made available to the incident response team in the event of a crisis. These people can be remote, supporting the organization over the internet or "in the cloud," or they can reside on-site and work side-by-side with the response team. In a situation where time is not on the organization's side and money is its only resource, having a team of people on-call who can help may be vital to organizational success.

Detecting and Responding to Incidents

Given that an organization is prepared for potential cyber incidents, the next step is knowing when an incident is occurring. Not all cyber events are incidents, and not all incidents come from cyber events. On one hand, cyberdefenses should tell an organization when many types of cyber events occur, from malware on computers, to malicious traffic on networks, to lockouts of accounts. On the other

hand, these types of events may occur every day and may not always constitute *incidents* that warrant special attention. An important part of "detecting" cyber incidents is sorting through all of the cyber activity going on in the organization, taking appropriate action for the activity, and involving the right people within the organization in those actions.

This section considers some of the topics regarding how an organization can identify cyber incidents within its environment and how it may determine when a cyber event warrants activation of formal incident response processes. These topics are shown in Figure 13.3.

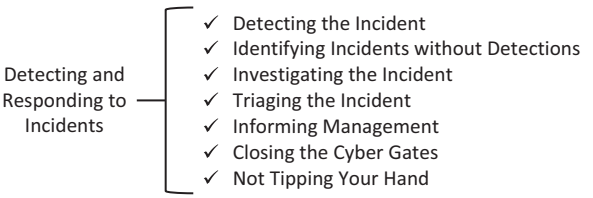


Figure 13.3: Detecting and responding to incidents includes cyber investigation, triage, reporting, and initiating containment.

Detecting the Incident

One of the easiest ways to identify an incident is to detect it through the organization's detective controls or its outsourced managed security services (MSS) provider. However, not all detections constitute incidents. Based upon the cyber events detected, an organization will need to set thresholds and establish guidelines for the activation of cyber incident response processes. These thresholds require some level of investigation to understand what is going on before an incident can be declared.

Identifying Incidents without Detections

Other incidents may be identified without direct detection. For example, incidents may be brought to an organization's attention by its business partners, service providers, customers, banks, credit card processors, or law enforcement. In these cases, they will likely bring the organization a claim that "You have been hacked, because . . . "

Hopefully, the claims are backed up by some number of facts or assertions that can be easily verified and further investigated. In other cases, the claims are difficult to verify or investigate (or may be false or incorrect). Such claims can lead organizational cyber response teams on difficult and time-consuming investigations to try to understand what has actually occurred.

Investigating the Incident

Once the event or incident has been brought to an organization's attention, it needs to investigate the incident to understand what actually happened, what potential business consequences are, and what level of response is appropriate to the situation. A particular challenge in this situation is that investigations take time and a fast-moving cyberattack or malware outbreak may occur faster than people are able to investigate. The organization's response team needs to use judgment when investigating the incident, estimating the risks involved, and recommending actions to IT, management, and the rest of the organization.

Triaging the Incident

As an organization investigates the incident, initial actions to address the cyberattack may be obvious, such as the following:

- If there is malware or malicious network traffic related to a single computer, it may be appropriate to isolate that computer and arrange for its cleanup, re-imaging, or replacement.
- If there is malicious activity associated with a single user account, it may be appropriate to reset the account's credentials, disable it from being used, or remove the account altogether.

On the other hand, if the activity involves multiple computers, large amounts of network traffic, or many accounts, these types of steps may not be adequate or even appropriate.

Informing Management

Once an organization has an initial understanding of the situation, it should inform management of what is occurring or has occurred. This reporting should

include the scope and business ramifications of the cyber events that were detected by cyberdefenses, or that were reported to the organization by others.

If the incident was minor, this reporting may be as simple as an e-mail documenting what happened and what was done about it. If the incident was not minor, this reporting will likely include preliminary assessments of the business damage that occurred, speculation on what is known and what is still unknown, and recommendations for activating the incident response process.

Closing the Cyber Gates

When an initial assessment of the situation is complete, the organization can go about responding to the larger business situation. This response is highly dependent on the business consequences of the cyber activity that occurred, and the business impact of responding to the attack. Malware on a dozen computers may not be much of a concern, unless one of those computers belongs to an executive or is being used to control plant production.

On the other hand, among critical business systems, even a minor anomaly can be of tremendous concern. In this situation, it may be prudent to "close the cyber gates" and put the organization into a more defensive or more protected cybersecurity posture. Such activities may include isolating critical production or operations networks from general IT networks, disabling wireless access or virtual private network (VPN) connections, or disconnecting from the internet altogether. These types of actions are intended to slow the spread of malware infections, reduce attackers' ability to operate inside an organization's environment, and protect critical operational functions.

Not Tipping Your Hand

At the same time that an organization may be adjusting its cyberdefenses posture in response to an attack, it should be aware that the attackers may be able to adjust as well. When battling professional cyberattackers – which includes cyber criminals, nation-state attackers, and industrial hackers – the attackers may be watching for the organization's response and have their own contingency plans. These attacker contingency plans may include alternative channels for command and control (C&C) and additional compromised accounts, computers, or software that the organization may not know about.

Against this type of cyber adversary, it may be prudent to take a moment and think through what the attacker's next step might be after the organization's initial response. An organization does not want to tip its hand with an incomplete or poorly thought-out initial response. An organization could end up playing "whack-a-mole," where it is constantly one step behind the attacker as the attacker moves around its IT environment.

Reporting to Management and Employees

As an organizational cyber incident develops, it is prudent to report to management what is going on so they can understand the situation and provide necessary support and guidance. Management also needs to be informed if cyberdefense activities are going to result in actions – like disabling computers, accounts, or network connectivity – that may impact the organization's business. In cases where business activities are impacted, it may also be necessary to inform employees, contractors, or business partners of the activities underway and their potential impacts. This communication is critically important.

Failures in cyber incident communications can be more damaging to internal business relationships than the consequences of the incidents themselves.

Clear communication involves collecting objective information about the situation and cyber status, reporting the facts and relevant analysis, and providing clear and actionable guidance to affected parties.

This section considers some of the topics regarding how an organization's cyber department can clearly communicate to the rest of the organization while handling a cyber incident. These topics are shown in Figure 13.4.

Figure 13.4: Reporting to management and employees involves delivering clear communications to the stakeholders of a cyber incident, in the midst of an uncertain and rapidly changing situation.

Data Collection

The first step in effective cyber incident communications is collecting the facts that are known about the situation. This data collection may include data about specific computers, devices, applications, databases, networks, facilities, accounts, or people involved in the incident. It is important to keep track of this data along with when and where specific data elements were discovered or determined. One technique is to keep a log of new information as it becomes known, or to document relevant details in e-mails or other internal communications. As data changes or errors are discovered, it will be important to keep track of when the situation changed or the new information became available, along with its impact on the incident response effort.

Facts, Analysis, and Speculation

It is also important to distinguish among facts, analysis of the facts, and speculation. Speculation and misinterpretation of the available facts are common sources of confusion. The problem is that in a rapidly changing situation, information often gets passed on second-hand and third-hand, particularly as it is summarized for higher levels of management. Facts can easily get distorted when they are intermingled with guesses and then summarized by personnel not directly involved or aware of the actual situation. It is okay to speculate, but make sure the speculation is kept separate from the facts.

Messages should clearly separate "what we know" from "what we think." Also problematic are technical details devoid of context or explanation. Telling people that a particular executable file was found running on one of the organization's computers does not have much meaning until it is also explained that the file contains malware and represents an active cyberattack.

Initial Reporting

Once the initial data about the situation is collected and some facts are known, the next step is to report those facts to management and other affected parties. In these initial reports, it is important to include context and meaning, while also separating out the facts from analysis and speculation derived from the facts. Avoid vague statements that are easy to misinterpret and sensationalize, such as "the data center has been compromised." Instead, separate reports into the facts, interpretation of the facts, and the potential business consequences.

Also, clearly point out what is *not known* along with what investigations are underway to find out more.

If some action is necessary in response to the situation, share that information, along with decision points on how the organization can decide whether to act or not. If there are many facts, include an executive summary that contains a "sound bite" version of the situation for busy senior leaders. It is helpful for such summaries to be drafted by those knowledgeable of the situation, rather than by senior managers who may not understand the details or what those details really mean to the business. Middle managers can work with technical staff to draft both a detailed version of the report and a "one sentence summary" for the executives.

Leadership Decisions

Often, these initial reports are precursors to leadership decisions regarding actions to take, tradeoffs to manage, resources to assign, or communications to disseminate. Simply asking management what the organization is supposed to do is probably not the best strategy in a difficult cyber situation. It is usually prudent to do some decision analysis first. This decision analysis should include identifying the possible actions to take, the potential consequences and ramifications of taking those actions, and how the situation might change in response to the actions being taken.

Winnowing down the range of possible actions – the possibilities are usually endless – to between two and five viable courses of action tends to be helpful. It is also helpful to analyze those courses of action in terms of their potential consequences, tradeoffs, and costs. Because there is an adversary involved, it is important to consider what the attacker might do in response to the organization's actions, and how the attacker's response might affect subsequent options for organizational response.

Legal Reviews

Frequently, cyber incidents result in situations with ramifications that might be of interest to an organization's legal department. Contracts, personnel, and regulatory compliance may all be affected by an incident. When this situation is the case, it is necessary to understand the scope, impact, and potential consequences involved, along with any applicable requirements for reporting or disclosure.

Even internal communications – particularly when disseminated to large numbers of employees – may need to be reviewed.

These internal reviews need to make sure that the communications do not disclose sensitive information, violate contractual requirements, or impact regulatory compliance. Also, cyber incidents may involve criminal activity that is of interest to law enforcement, or that requires safeguarding of evidence, forensics, or other pertinent data. For all of these reasons, Legal should be involved early and often in the cyber incident process. They should be given the opportunity to regularly review the situation and any applicable supporting materials, and their inputs should be solicited when making decisions.

Employee Communications

Smaller cyber incidents – perhaps affecting just a few computers, devices, or accounts – may be handled internally by the cybersecurity department or in collaboration with the organization's IT department. Larger cyber incidents that affect larger numbers of people, or external parties such as customers or business partners, may require additional coordination and handling. Communications with employees should be given attention, particularly if they are going to more than a few employees or to employees not directly involved in the cyber incident itself. Such employee communications may be drafted by internal human resources (HR) or communications personnel, and should probably be reviewed by legal as well.

Messages to employees should be carefully prepared to contain only the facts that are relevant, to avoid extraneous details or speculation, and to focus on the information that employees should know and the actions that employees should perform. Messaging may include warnings to not talk to the press, customers, or other external parties about what is going on, and to defer inquiries from external parties to official channels. Even though these communications are supposed to be internal and proprietary, an organization should draft them assuming that they will be publicly disclosed. Memos leak, particularly when they are about cyber incidents. Keep messaging succinct, professional, and solution-oriented.

Revisions and Clarifications

As the situation develops, an organization may find itself discovering new facts, reinterpreting previously known facts, or analyzing the situation in new

ways. The organization may also find the situation evolving, particularly if it is dealing with an attacker who is actively operating within the IT environment. An organization may also discover that what it thought it knew turned out to be incorrect or that its analysis was faulty. Initial reports often turn out to be wrong or at least incomplete. This situation can make it necessary to issue revised reports, make revised recommendations, change the course of action, or provide clarification to previously issued guidance.

When an organization revises reports, it should try to explain how the situation is evolving while avoiding making excuses for why previous reports may have been incorrect. Point out which facts have changed and how the analysis of the situation and recommendations going forward are changing based upon the changes to the facts. It is important to stay focused on the present situation and how it is evolving, rather than on the actions or mistakes that may be contributing to things getting better or worse.

Containing a Cyber Outbreak

Many of the most dangerous, most devastating, and most expensive cyber incidents involve large numbers of computers, accounts, databases, or other infrastructure within an organization's IT environment. Attackers may move laterally and escalate their privileges within the IT environment to get access to the "crown jewels" of customer data, proprietary technology, or financial accounts. Attackers may use scripts that deploy ransomware to hundreds or thousands of computers in a matter of minutes, or use remote access connections to exfiltrate gigabytes or terabytes of data from organizational systems and networks. Thanks to high speed networks and computers, much of this damage may occur before defenders even notice; or if they do notice, faster than they can respond.

If an organization detects these activities while they are in progress, it may be able to stop attackers from accomplishing their objectives, but only if the organization can move quickly and decisively in its response. When an organization has the good fortune to catch an attack that is underway but not yet complete, it will need to move quickly and decisively to stop the attackers before they can achieve their objective. Unfortunately, attackers seldom announce their intentions and the fact that the attack is still in progress may not be obvious. Analysis, interpretation, and speculation will likely be required to ascertain the attackers' intentions, along with after-the-fact forensic investigation.

This section considers some of the topics an organization should consider when containing a cyber incident or outbreak that is in progress when it is discovered. This includes describing how an organization can identify an attack

that may not yet be complete, and the steps it may need to take to counter an active attacker who could try to elude a defensive response. These topics are shown in Figure 13.5.

Figure 13.5: Containing a cyber outbreak involves taking the advantage away from the attacker and regaining control of the IT environment.

Defending Along the Kill Chain

To understand how far along attackers are in their attacks, it is helpful to consider the steps of the cyber kill chain or attack sequence.[3] Consider the following examples of where an attacker is in the attack sequence:

- If an organization has malware on an endpoint that the user believes was caused by opening an e-mail attachment or web link, then the attack is likely early in the sequence, near the "foothold" stage of the attack.
- On the other hand, if an organization finds malicious activity related to a system that does not normally connect directly to the internet, then it is possible that the attacker is in the process of lateral movement within the organization.
- If an organization is investigating suspicious administrator account activity, then the attacker may be in the process of escalating their privileges.
- If an organization is investigating "unusual" activity on database systems, file shares, or critical business applications, then the attacker may be in the process of accomplishing their end-goal objectives.
- If an organization is investigating large data flows that exited its networks, ransomware, or other malware on a large number of its servers or endpoints, then the attack may have succeeded and it is simply too late.

3 *Kill chain* or *attack sequence* refers to the steps a cyberattacker takes to conduct an attack to compromise the confidentiality, integrity, or availability of the victim. See Chapter 10, "Organization Cyber Awareness," for the description of a five-step cyberattack sequence that cyberattackers commonly follow when penetrating organization cyberdefenses.

An attacker does not use just "one set" of attack sequence steps to take control of computers and accounts inside an organization. However, it is helpful to understand the steps required for various types of attacks to succeed. By focusing on how attacks usually occur, organizations can design defenses that disrupt, detect, delay, and defeat the attacks after they start, but before they can succeed. Each attack step is an opportunity for cyberdefense to deliver protections to an organization.

Finding the Attackers in Your Midst

As an organization investigates an attack, it will likely find indicators of compromise (IOCs) as well as tools, techniques, and procedures (TTPs) used by the attackers. It may also see signs of attacker command and control (C&C) network traffic, although that traffic will likely be encrypted and difficult to analyze. By examining the logs of affected systems, and searching the IT environment for IOCs, TTPs, and C&C, an organization can probably identify where the attackers are operating in the IT environment, and where they are coming from. With this identification, an organization can estimate which computers, devices, networks, and user accounts are involved in the presently occurring cyberattack.

Isolating Computers, Devices, Networks, and Accounts

When an organization is ready to counter the attack, it should act quickly to isolate the affected computers, devices, networks, and accounts. The goal here is to repel the attackers from the IT environment all at once, before they can respond. One cyberdefense technique is to disconnect the entire organization from the internet – or at least block most of its internet access – while the cleanup occurs. This makes it difficult for attackers to change over their connections to the enterprise to use backup malware or control channels. Another cyberdefense technique is to write scripts to perform the cleanup, so that the cleanup can execute quickly at machine speed. Either way, the goal is to repel the attackers faster than they can respond and take evasive maneuvers. This includes simultaneously denying their access to organizational computers, networks, and accounts.

Plugging Defensive Holes

As an organization is chasing down the attackers' footholds in its IT environment, it will also want to bolster its cyberdefenses to keep the attackers out. One question an organization should answer is the following:

Did the attackers get in by taking advantage of specific vulnerabilities, missing patches, defensive design flaws, or open back doors?

If the answer is yes, then the identified gaps should be addressed at the same time that the organization is repelling the attackers. Where the vulnerabilities cannot be remediated directly, perhaps an organization can compensate with additional monitoring to catch if the vulnerabilities are exploited again. An organization does not want to go to a great effort to remove attackers only to find them back inside its environment the next day using the same IOCs, TTPs, and C&C channels.

Monitoring Lingering Access, Strike, and Counter-Strike

Attackers may have some "tricks" up their sleeves, including backup communications links and alternate C&C channels into an organization's IT environment. Attackers may also have tool sets deployed that an organization is not aware of, malware that it has not yet discovered, or footholds in internet-facing systems that it did not catch.

If these attacker "tricks" are present in the IT environment, then an organization can expect that its defensive strikes against the attackers will be met with attacker counter-strikes. Attacker counter-strikes will leverage these additional tools and connections so that the attackers can maintain their penetration of organizational defenses. As an organization seeks to defeat initial attacks, it should monitor its IT environment carefully for additional signs of malicious activities. With this monitoring, the organization should be prepared to quickly pivot to repel other attacks as they are discovered.

Anticipating Dangerous Escalation

If the attackers have additional footholds, tools, accounts, or devices at their disposal, then they will likely use them to try to maintain their position and press the attack. The attackers may also dramatically accelerate their activity, since they know they have been detected and time is no longer on their side. In addition, at this point in the attack, they may dramatically escalate their attack

or take actions that are destructive to an organization's IT environment. The attackers may launch scripts seeking to overload an organization's network or disable its systems to distract cyberdefenders and buy the attackers more time to finish achieving their objectives. Faced with potential defeat, the attackers may believe they have nothing to lose by striking back at their victim – the organization – and using cyber destruction to cover their tracks.

Protecting Critical Assets from Collateral Damage

Between the attacker's activities and an organization's efforts to counter them, there will likely be collateral damage that occurs against organizational IT systems. Computers may have to be re-imaged, network-connected devices may be disconnected, user accounts may be disabled, and network addresses may be blocked. If the attacker unleashes ransomware or takes other destructive actions against an organization, the potential damage may be considerable. This damage can even include physical destruction of manufacturing capabilities, network-connected operational technology (OT) controlling physical equipment, or healthcare systems. Before embarking to remove cyberattackers from its IT environment, an organization should consider these possibilities, understand the risks to safety and the business, and take measures to protect its most critical assets from potential harm.

Changing Passwords

One process that tends to be at the heart of an incident response is "password reset." Changing the password of a single account or even a group of accounts is usually straightforward. The problem is that in many cases of cyber incidents, the prudent action is to change *all organizational passwords*, or at least all of the passwords stored in a specific directory, database, or authentication system. For internal systems like Microsoft's Active Directory, password reset can mean changing all employee, administrator, and system account passwords. For customer-facing organizational systems, password reset can mean asking all customers to change their passwords.

There are many challenges with doing mass password resets. While authentication systems can generally handle the workload of changing thousands of passwords simultaneously, the effort can place a tremendous strain on communications teams and support staff trying to manage all of the related support calls. Even if only 1 in 10 users in a large organization (or its customer base)

requires hands-on customer support for a password change, the workload can rapidly become untenable with thousands of support calls all coming in at approximately the same time.

For enterprise systems, password changes of disconnected or remote users can require multiple steps like virtual private network (VPN) connections or updating of system configurations. Credentials cached in applications, browsers, operating systems, and mobile devices can cause large numbers of login attempts using the old passwords and potentially lock accounts. If an organization has a strict account lockout policy – such as fewer than 5 password attempts before the account locks – it may want to consider relaxing the policy during the password reset period.

Other password reset challenges include how to handle accounts that never get updated. *Is there a good reason why such accounts have not had their password changed? Or are they really "zombie"*[4] *accounts that should have been deleted anyway?* The password reset effort will likely reveal or exacerbate issues and challenges within an organization's identity management systems.

This section considers some of the topics an organization should consider regarding its password management and password reset process. This includes how passwords are typically stored and protected, how they become compromised, and some of the specific nuances in changing passwords for different types of users. These topics are shown in in Figure 13.6.

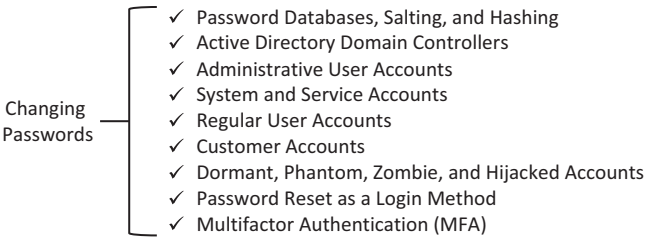


Figure 13.6: Changing passwords involves positioning the organization to conduct a password reset by understanding the challenges associated with changing large numbers of organizational passwords due to a cyber incident.

4 A zombie account is an account that has been abandoned by its user and is no longer actively being used. However, because the account was never closed or de-provisioned, it may be taken over by attackers using large databases of compromised user credentials.

Password Databases, Salting, and Hashing

An important initial factor to consider is where the passwords are stored and how they are protected. For custom enterprise applications, particularly proprietary customer-facing ones, organization applications may be storing user passwords in their own databases. For protection, these databases should be access-controlled, encrypted, and store salted password hashes,[5] rather than plain-text passwords. Storing password hashes involves storing a hash of the password, rather than the password itself. Hashes are one-way functions that prevent a person from knowing the plain-text password, even if the person can read the database. Salting the password with a random value before it is hashed ensures that the hash value is unique even if two users have the same password. These protections make it more difficult for attackers to compromise users' credentials, even if the attackers can get to organizational password databases.

Active Directory Domain Controllers

Microsoft's Active Directory is the most common on-premise enterprise directory in common use, and is likely used to manage an organization's user, administrator, and system accounts and credentials. Active Directory uses a multi-master database hosted on domain controller servers to provide enterprise authentication using lightweight directory access protocol (LDAP). While it is based on open standards, Active Directory has many Microsoft-specific customizations and quirks. It also is a top target among professional cyberattackers who try to exploit it to take control of an organization's IT enterprise. To guard against these attacks, Active Directory must be specifically hardened against attacks exploiting Windows operating system vulnerabilities, targeting protocol vulnerabilities like Pass-the-Hash, compromising Domain Administrator account credentials, and using tools like PSExec to distribute malicious software.

Administrative User Accounts

Once organizational authentication databases and enterprise directories are protected, the next step in a password reset effort is to reset administrator

5 Salted password hashes are a form of password encoding.

credentials. These credentials should be an organization's highest priority, as these are the accounts that attackers target to compromise an organization's infrastructure. These accounts include directory administrators, application administrators, and endpoint administrators. They may also include local administrator accounts on endpoints and servers. Local administrator accounts can be particularly tricky to change because they are local to specific devices and may not be centrally managed by the organization. Fortunately, forcing password resets among system administrators should be relatively easy because there are few of them and they tend to be understanding of security issues.

Unfortunately, username/password authentication may not be adequate protection for the most sensitive accounts. For administrative accounts, an organization should seriously consider putting dynamic password management in place – changing passwords frequently or even every time accounts are used – along with multifactor authentication. Finally, as a part of this password reset effort, an organization should conduct an audit of its administrative accounts to verify that accounts are needed, that they have required permissions (and not excess permissions), and that their activity histories do not contain signs of abuse.

System and Service Accounts

These accounts are used for applications, services, and servers within an organization to interact with each other. Sometimes these accounts have powerful administrative privileges. While administrator accounts are obvious targets for attackers who want to escalate their privileges, system and service accounts tend to be not-so-obvious targets and are potential vulnerabilities. Service accounts may be able to create other accounts, assign privileges, log in to endpoints, or control cloud applications. Because these accounts are embedded into organizational IT applications and systems, they may be difficult to understand, maintain, or change.

Changing the password on a service account may require updating tens or hundreds of scripts where the password is embedded. It may also require taking key systems – such as financial, manufacturing, or patient care – offline to do the change. In many cases, the operational impact of such a change is unacceptable, even against the risk of account compromise or abuse. Password changes for these types of accounts will likely need to be handled on a case-by-case basis, with every account being individually considered and handled. For service and system accounts that cannot have their passwords changed, an

organization should consider compensating controls like limiting their privileges and permissions, isolating their use to just specific networks or devices, and monitoring to trigger alarms if there are signs the accounts are being abused.

Regular User Accounts

Once administrator and system accounts are addressed, the next group to worry about is regular users. While generally less sensitive than highly privileged accounts, regular user accounts can still be highly sensitive, especially when they belong to senior executives, financial operators, or IT administrators. For larger organizations, it may not be practical to force all users to change their passwords simultaneously. An organization may want to break the effort up into batches spread out over a couple of days, or even a week or more. When an organization creates those batches, it may want to reduce its overall risk by grouping accounts so that the most important, sensitive, and vulnerable user accounts are reset first.

When doing mass password resets, an organization needs to manage communications with its users, indicating when they will have to change their passwords and how to do it. An organization also needs to give special consideration to users who are remote – those working from client sites, on travel, on vacation, or otherwise disconnected. It is necessary to think through what will happen to users who do not change their passwords on time and whose accounts get locked out. *Will they be able to communicate with the organization to regain their access?* Finally, it is necessary to think through what happens after the password reset, when all of the simultaneously changed passwords expire again and are ready for their next regularly scheduled update. An organization may want to adjust its password update policies, so that future scheduled password changes are spread out. The organization does not want to end up with *another* wave of password expirations only 90 or 180 days after the original password reset!

Customer Accounts

Resetting passwords on customer accounts brings about another set of challenges. Generally, customer password resets and employee password resets use different underlying systems and credential databases. In a cyberattack, it may be possible that an organization will only need to do one or the other. Customer account password resets should only be necessary if customer authentication

systems are compromised or if the organization gets feedback that large numbers of customer accounts have been compromised.

With customer account password changes, an organization needs to tread carefully, because these accounts belong to customers and/or business partners. When an organization forces a customer password reset, some customers are never going to come back or are going to end up creating entirely new accounts rather than go through the password reset process on their old accounts. Customers may require significant support to get cached passwords updated on browsers, computers, mobile devices, and smart appliances. Also, customer communications and password checks via e-mail will likely generate large numbers of failures, possibly indicating dormant, phantom, zombie, or hijacked accounts.

Dormant, Phantom, Zombie, and Hijacked Accounts

In an organization's password reset effort, it will likely find signs of accounts that are no longer in use, were not created legitimately, are being used after the legitimate user thought the accounts were disabled, or that have been taken over without the user's knowledge. While this situation occurs primarily with bank accounts, it can occur for other kinds of online accounts as well. Some different types of problematic accounts are as follows:

- *Dormant accounts* are accounts that are still in place, but are no longer being used or monitored by the user. They may also be tied to e-mail accounts (particularly work accounts) that are no longer active or being used.
- *Phantom accounts* are accounts that were created in users' names, but without their knowledge, particularly as a part of identity theft.
- *Zombie accounts* are accounts that the user thought were closed or dormant, but which have been taken over by someone, usually for identity theft or fraud.
- *Hijacked accounts* are legitimate accounts that the user is actively using, but which attackers are also using. This situation frequently occurs for e-mail accounts, also as part of identity theft.

Because password resets require the credentials on these accounts to be updated everywhere they are being used, they can reveal many of these issues and may result in some difficult calls from upset customers or users. In particular, a password reset should prompt an organization to think carefully about its account expiry and deletion process. Emerging privacy regulations place strict penalties

on compromised user accounts and may require an organization to be proactive in removing accounts that are no longer needed or used by its customers.

Password Reset as a Login Method

When dealing with a password reset, an organization should also consider its password change and password reset processes. All of us know people who cannot remember their passwords, and either have stored them in the browser or use the password reset function when logging in almost every time!

For accounts that are used only occasionally and that have strict password complexity policies, password reset may become the primary method of authentication for large numbers of users. For internal user accounts, an organization may have a self-service password reset based on multiple personal questions or multifactor authentication tokens. For external customer accounts, an organization's self-service password reset will likely be based on user e-mail accounts, personal mobile devices, or identity verification services such as ID.me.[6] An organization should carefully analyze these processes and consider how they fit together with its password reset mechanism as part of a holistic user identity verification and authentication solution.

Multifactor Authentication (MFA)

The pain of an organization or customer password reset may make the cost of multifactor authentication (MFA) seem a little more palatable than it might have been before a cyber incident. MFA remains one of the strongest security measures an organization can put in place to counter hacking against its networks, computers, and IT systems. While MFA is complex and expensive, today's MFA technologies use mobile, biometrics, and adaptive authentication – along with cloud-based and cloud-first protocols like security assertion markup language (SAML)[7] and OAuth[8] – to deliver a seamless solution that is plug-and-play for many applications.

---

6 See https://www.id.me/: "ID.me provides secure identity proofing, authentication, and group affiliation verification for government and businesses across sectors."

7 Security Assertion Markup Language (SAML) is a standard for exchanging security credentials between different organizations' security domains.

8 OAuth is a standard that enables users to allow websites or applications access to their information without using their passwords.

Organizations should consider using some level of MFA for access to internet-based systems, cloud applications, and privileged administrator accounts. Organizations should also enforce MFA for user accounts that can handle large amounts of money – like banking or e-commerce accounts – as well as internal accounts with access to financial systems. While not impenetrable by any means, MFA is effective and should be part of the foundation to an organization's overall cyber defense posture.

Managing a Cyber Crisis

Sometimes, a cyber situation escalates to the point where it is no longer merely an incident, but has instead become a crisis. A cyber incident becomes a crisis when it has a widespread or significant effect and jeopardizes people, equipment, facilities, or the organization's ongoing operations. When a situation becomes a crisis, it goes from being "merely" an IT problem to being an organizational problem that may be of existential importance. For example, when Saudi Aramco had over 30,000 computers disabled by cyberattackers, it was a crisis. When Medstar had to turn patients away because its networks had been taken down by ransomware, it was a crisis. When Maersk Shipping was unable to load or unload ships because IT systems were unavailable, it was a crisis.

Crisis situations tend to be fundamentally different from "normal" cyber incident responses. As Murphy's Law of Combat once stated, "You know you are in combat when you are short on everything except enemy." In a crisis situation, an organization will likely be operating within IT environments that are highly impaired and unable to provide expected IT capabilities. This impairment may be due to ransomware or other attacker actions, or may be caused by an organization's attempts to defend against an attack in progress.

These impaired IT resources may deny an organization the ability to collaborate, communicate, operate, or administer systems under normal circumstances. An organization may even get "locked out" of parts of its own IT environment because accounts are disabled, passwords are changed, networks are disconnected, or key reference documents are unavailable. In today's decentralized but highly connected IT environments, it is easy for things to get broken in ways that are difficult to repair.

This section considers some of the topics an organization should consider regarding cyber crisis situations and how they tend to be different from normal cyber incident responses. This includes techniques for operating while in crisis and resources an organization should be prepared to employ for additional assistance. These topics are shown in in Figure 13.7.

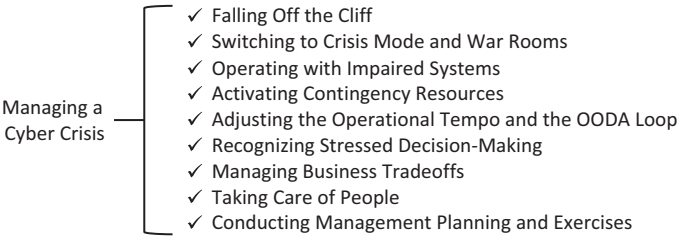


Figure 13.7: Managing a cyber crisis involves transitioning to "crisis mode," so an organization can respond quickly and effectively to a difficult situation, while simultaneously taking care of its business and its employees.

Falling Off the Cliff

Frequently, a cyber crisis starts with what some cyber professionals refer to as "falling off the cliff." This situation is the point where defenders realize that the situation is no longer just a case of a couple compromised computers or accounts, or some malicious network traffic. Consider the following cases:

- Perhaps attackers have taken control of a critical administrator account or are accessing a key server, database, or cloud service.
- Maybe malicious network traffic is no longer isolated, but has spread throughout the organization's networks or internet connections.
- Maybe the situation has gone from a couple of anomalies or alerts to a full-blown ransomware outbreak.

In these types of cases, the realization that things have become very bad occurs very quickly, and an organization will struggle to keep up as the crisis situation continues developing and evolving.

Switching to Crisis Mode and War Rooms

Once an organization understands that it is in a crisis situation, it is well-served to switch to "crisis mode" as quickly as possible. This conversion should include dusting off the "crisis management" section of the incident management or disaster recovery plans. Switching to crisis mode should involve specific management communications and decisions to alert the organization that it is no longer just battling an incident, but may be battling for its survival.

At this point, it may be helpful to bring key leaders together in a "war room" environment so that everyone can coordinate and understand the

rapidly changing situation. In organizations where people are decentralized, this coordination may be accomplished with virtual war rooms, conference calls, or online collaboration tools. So newcomers can rapidly come up to speed on the present situation and the latest developments, it can be helpful to have physical or virtual whiteboards and document repositories.

Operating with Impaired Systems

In a crisis situation, it is likely that some of the organization's business systems will be taken offline, disconnected, or otherwise impaired. This situation may be due to actions by the attacker or may be a part of organizational defenses to counter the attacker and reduce their potential damage. Defensive measures may include disabling virtual private network (VPN) remote access, severing wide area network (WAN) connections, isolating data centers, disconnecting manufacturing networks, or locking out user accounts. Attack consequences may include ransomware on endpoints or servers, corrupted data, disabled applications, or other IT damage. The most dangerous attacks may even include damage to physical systems through their control systems, programmable logic arrays (PLAs),[9] or through malicious control instructions. This damage may take out collaboration tools like e-mail, messaging, file shares, or intranet sites. It may also take out video conferencing, telephones, or even facility heating, ventilation, and air conditioning (HVAC) systems.

Activating Contingency Resources

When an organization's primary systems are impaired, it may be prudent to activate contingency resources. These contingency resources can be used to support the organization's response to the crisis, as well as its ongoing operations while resources are consumed responding to the crisis. Such contingency resources should be a part of the organization's crisis management and disaster recovery plans. Contingency resource plans may include satellite telephones, backup facilities, and alternate collaboration methods.

---

9 A *programmable logic array* (PLA) is like a miniature computer that can be programmed to process sensor data and direct operation of physical systems like plant machinery. Unlike general-purpose computers, they do not usually run operating systems or have user interfaces. Attackers can change their programming and cause the machines they control to malfunction.

If an organization's primary IT systems are offline, it may need to use personal IT resources to coordinate its personnel, including personal cell phones, computers, and internet services. An organization should not underestimate the power of Facebook, Twitter, Google Groups, or other free services for coordinating when primary business systems are offline. An organization may also need to activate contingency systems, backup data centers, or manual processes to keep its business operating. When an organization activates these contingency plans, it should also consider supplemental resources for its cyber incident response. The crisis might be a good time to activate the organization's "incident response retainer" and call in additional cyber expertise if such resources are available.

Adjusting the Operational Tempo and the Observe, Orient, Decide, Act (OODA) Loop

As the cyber crisis develops, an organization will find itself needing to process new developments, analyze options and tradeoffs, and make decisions about what to do next. A model for this activity is the OODA loop.[10] Simply stated, the OODA loop consists of the following four steps:

1. *Observe* the developing situation.
2. *Orient* to the situation based upon observations, knowledge, experience, and culture, and identify possible courses of action and tradeoffs.
3. *Decide* upon a course of action.
4. *Act* to put the decision into practice.

This decision-making process can help an organization determine how quickly it can respond to a changing situation. How often people meet to exchange information or make decisions becomes critical to how quickly the organization can process new information and change directions in response to a change in the situation. If response teams are only meeting once a week, then the organization is hard-pressed to quickly respond in less than a week.

In practice, it may take the organization several weeks to effectively respond if key meetings are only held once a week. Therefore, in a rapidly changing situation, it may be necessary for leaders to meet daily, twice a day, or even

10 U.S. Air Force Colonel John Boyd (1927–1997) developed the OODA loop to explain how fighter pilots perform in air combat. OODA has since been used as a model for decision-making under pressure for many types of adversarial situations.

continuously to be able to quickly process and respond to changes in the situation. This meeting frequency defines the organization's *operational tempo*, or how quickly it can maneuver against its adversary. This operational tempo it is driven by the OODA loop process, organizational structure, and the pace of the changing situation.

Recognizing Stressed Decision-Making

At the same time that an organization may be struggling to deal with a stressful cyber crisis, it will likely find key personnel to be overwhelmed and struggling. Consider the following stress factors at work during a crisis:

- In today's just-in-time, lean-organization world, organizations typically have little spare bandwidth among its systems or its employees to absorb any sort of adversity.
- There will be individuals with key skills or key knowledge who end up being at the center of the situation and whose bandwidth becomes a bottleneck to much of the entire organization's progress.
- The layers of middle management are likely to become saturated by the workload managing up and managing down, while senior executives and line workers sit idle.

This last bullet is particularly important, as it can have a huge impact on the organization's productivity in a crisis. In a crisis, an organization may find its workers sitting idle because they are unable to work due to disabled systems, or because they are waiting for detailed action plans on what to do from middle managers. Similarly, the organization may find its executives also sitting idle because they are waiting for reports or analysis from middle managers, or because they have given their strategic guidance and are waiting for middle managers to turn that guidance into action plans for the workers to execute. The end result of this is that the people in the middle are squeezed top-down as well as bottom-up. These overwhelmed middle managers' limited bandwidth results in the entire organization operating at a fraction of its potential capacity.

In addition, everyone is stressed further by the "fog of war," situational uncertainty, incomplete knowledge, and the need to make high-stakes decisions based on guesses and hunches. Organizations need to be aware of these stress factors and take actions to protect against them, including identifying overloaded key personnel and getting those personnel as much help as possible.

Managing Business Tradeoffs

As a part of this stressed decision-making situation, an organization will likely have to manage difficult business tradeoffs, such as the following:

- *Does the organization take its manufacturing line down for a day to install patches or to re-configure the network?*
- *Does the organization take its e-mail system offline because attackers are using it to infiltrate employee accounts?*
- *Does the organization disconnect from the internet to block attackers' command-and-control (C&C) activities?*
- *Does the organization send employees home because their computers are infected with ransomware?*
- *Does the organization pay employees while they are sitting idle?*

In many of these cases, the "best" choice from a cybersecurity perspective may not be the "best" choice from an IT perspective or from a business perspective. Cyber, IT, and the business will likely find themselves at odds with regard to each department's top priorities and preferences. Organizational leadership needs to be involved in understanding these preferences, the possible alternatives, the tradeoffs involved in each alternative, and the possible consequences should things "go wrong." These decisions can be difficult and expensive, particularly when potentially millions of dollars are involved.

Taking Care of People

As a stressful situation unfolds, an organization must keep an eye on the human element. In a cyber crisis or an IT recovery event, employees will likely find themselves in situations for which they were not trained, were not prepared, and were not expecting. An organization may ask its employees to work longer and harder than ever before, and potentially without regard to their other personal, family, or business obligations. While this situation may be acceptable for a couple of days, it likely will not be sustainable after a week or two. People will start burning out, and the last thing an organization wants is for star players to quit right in the middle of a difficult situation.

It is important for an organization to give thought to how it can take care of its employees, from top executives down to junior workers and contractors. Everyone will likely have important roles throughout the crisis. An organization can demonstrate its appreciation to the employees by catering lunch, bringing in laundry service, and arranging for childcare. As things drag on past the first

couple of weeks, an organization can think about "designated weekends off," happy hours, and night-out gift cards to help keep up employee morale. An organization should also consider retention plans for key personnel to incentivize them to stay with the organization until the crisis can be resolved.

Conducting Crisis Management Planning and Exercises

In crisis situations, one of the best ways to mitigate their organizational impacts is to think through potential crises beforehand. An organization should consider conducting cyber crisis management planning and response exercises. Such exercises can be conducted in conjunction with overall cyber incident response planning as part of IT hazard preparation or business continuity planning. Ideally, these exercises should be parts of all three activities, with different leadership teams thinking about the problems from their different perspectives.

Through these exercises, key business, IT, and cyber leaders can come together and agree on consistent ways for handling cyber crises across the entire organization. These processes enable leadership to understand the communications and decision-making channels involved – as well as the responses required – when dealing with a rapidly changing crisis situation.

Cleaning Up the Mess

As an organization gains the upper hand in its cyber crisis, it should find itself at a point where the end is in sight and it is time to "clean up" the incident or crisis "mess." This mess may include computers that need to be rebuilt or replaced, equipment that needs to be reconfigured, software that needs to be reinstalled or rewritten, and accounts that need to be reset or reprovisioned. This mess may also include vulnerabilities that need to be remediated to keep attackers out or to at least prevent them from immediately coming back. During the cleanup process, an organization may find itself needing additional resources to "bridge the gap" while capabilities are reconfigured, backups are restored, or forensics are performed.

This section considers some of the topics an organization should consider when cleaning up a cyberattack and restoring normal operations. This can include considering how an organization may restore its operational capabilities, while also defining a new "normal" going forward after a crisis event. These topics are shown in Figure 13.8.

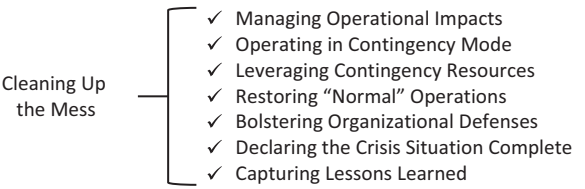


Figure 13.8: Cleaning up the mess involves taking multiple steps to restore normal operations and reinforce the organization's cyberdefenses, while also capturing lessons learned for the future.

Managing Operational Impacts

During recovery, there will likely be operational impacts. Primary IT systems may be offline, critical cloud services may be unavailable, or organization networks may be disabled. These impacts need to be managed so that the organization can continue functioning and responding to the crisis. Managing operational impacts – particularly those caused by responses to the attack, rather than the attack itself – is going to be challenging.

Remember that the *Apollo* space missions[11] went to the moon on less computing power than today's smartwatch – even small-scale computers can produce significant results! For example, today's IT professionals are used to having racks and racks of computers, each doing specialized tasks. However, it may be possible for an organization to run its whole manufacturing line off of a laptop if all the bells and whistles are temporarily disabled. Disabling logging, reporting, analytics, or other diagnostic functions may enable production applications to run on a fraction of their usual computing requirements.

Similarly, an organizational website that normally requires a dozen servers may be hosted on a single underpowered server if the graphics, sound, videos, and advertisements are disabled. The website may not look great, but at least it will be working. Technical employees will likely have many good ideas about where "corners can be cut" to enable production to continue, even though primary IT systems may be impaired or unavailable. Ideally, such ideas should be worked out ahead of time, and be a part of the organization's formal contingency plans.

11 United States' *Apollo 11* landed on the moon on July 20, 1969.

Operating in Contingency Mode

Just as employees need to get creative to manage the operational impacts of crisis-related IT issues, they will have to get equally creative to keep IT systems operating in "contingency mode." This situation may involve activating backup facilities, data centers, cloud providers, or application servers. An organization may find itself restoring from backups, activating alternate service providers, or trying out the concept of using the test systems for production – an idea that is often discussed but seldom actually tested.

Operating in a contingency mode requires an organization to think through alternative solutions requiring creative but realistic approaches. To think through feasible contingency strategies, an organization should consider questions such as the following:

- *What IT systems can the organization operate using backup computers, personal computers, or mobile devices?*
- *Can the organization rent additional IT systems or hire a service while its primary systems are offline?*
- *If the data center is unavailable, can the organization use cloud services?*
- *Can the organization stand up an open-source database to give employees basic capabilities and reporting while the organization's primary system is being rebuilt?*

It is important to be creative while thinking through alternative solutions. Many low-cost solutions may be possible, but require "out-of-the-box" thinking.

Leveraging Contingency Resources

As a part of operating in emergency mode, an organization will likely need to activate contingency resources. Primary systems may be tied up for forensics, resynchronizing storage arrays, or restoring systems and data from backups. Backup systems may be needed to test restoration procedures or perform much-needed emergency upgrades. Assuming organizational resources were operating at maximum capacity before the crisis occurred, restructuring to recover from the crisis will likely require vastly more resources than are available. An organization needs to be prepared to make tough decisions about repurposing available resources or obtaining additional resources. For example, decisions may include answering the following questions:

- *Can the organization rent additional computers, software, or licenses?*
- *Can the organization leverage cloud-based infrastructure or switch over to its backup site to be the primary?*

Cloud-based applications and infrastructure can be game-changers, as hundreds or even thousands of servers can be stood up in minutes by using nothing more than a credit card and a couple lines of code. An even better approach would be to have such code written, tested, and standing by in case of an emergency.

Restoring "Normal" Operations

Eventually, an organization should be able to recover its capabilities to the extent that "normal" operations can resume. This recovery process often occurs in phases as things return to normal for different parts of the organization.

1. *Manufacturing and business operations* will likely be restored first, as it is imperative that they be brought back to full operating (and revenue-generating) capability as quickly as possible.
2. *Business back-office operations* may be the next systems to be restored because they provide the functions that enable the business to operate – paying bills, billing customers, and tracking the business's finances.
3. *IT* may be next to restore "normal" operations, although it may take some time from when the business resumes normalcy until IT is actually restored to its full operating capacity.
4. *Cybersecurity* will likely get back to normal sometime after IT, although cybersecurity may continue working for some time to further bolster the organization's cyberdefenses.

Hopefully, the cybersecurity strengthening will occur within the framework of normal cyber projects and initiatives. Most likely, the last department to get back to normal will be the organization's legal team, as regulator actions, legal mitigations, and litigation may stretch on for years after the actual cyber crisis has been completed.

Bolstering Organizational Defenses

As the crisis situation winds down, an organization may find itself bolstering its cyberdefenses to make sure such a crisis will never happen again. Beware

the temptation to lock things down so far that cybersecurity gets in the way of the organization's operations and hampers productivity. Certainly, an organization should take advantage of the opportunity to address critical gaps, improve visibility, or restructure its cyberdefenses to better align with organizational objectives.

An organization should use the crisis as an opportunity to take another look at its cyberdefenses, perhaps from a different perspective than before. The incident probably did not escalate into a crisis because of one "critical flaw" in the organization's cyberdefenses. If one flaw is enough to bring down the entire organization's cyberdefenses, then its cyberdefenses are probably not robust enough. An organization should look carefully at its cyberdefense architecture and consider how it can have at least two layers of defenses – along with multiple alarms – that will have to be defeated before a crisis can occur. While restructuring and layering cyberdefenses may not be possible for every IT system or data element, it should be seriously considered for the most important ones.

Declaring the Crisis Situation Complete

As the cyber crisis winds down, it will be important to formally declare the end of the crisis and the resumption of "normal" business. This transition may occur at different times for different teams and for different parts of the organization. An important factor to consider here is financial. The crisis may have distinct accounting from regular business operations, and crisis-related costs may need to be itemized and tracked separately. This accounting may be simply because business leadership wants to understand the costs of dealing with the situation, or it may be because all or some of the costs are being paid for by insurance, business partners, or other interested parties. Organizational leadership should provide clear guidance here – based on the applicable agreements and contracts – to limit both the scope and the time period of the costs involved.

Capturing Lessons Learned

At the end of the crisis situation, an organization will likely have learned many lessons for how it would like to do things better "next time." While the organization hopes there will never be a next time, it is important to capture at least some lessons learned and incorporate them into the organization's culture going forward. It is useful to conduct lessons-learned sessions with key team

members while their experiences are still fresh, and to take written notes about their experiences.

While standalone lessons-learned documents may be useful, they may be quickly lost and forgotten as busy employees get on with their jobs and lives. It may be more impactful to incorporate lessons learned into the organization's institutional knowledge, operational processes, and contingency plans. A section of "do's" and "don'ts" at the back of the organization's incident management plan – based upon lessons learned from the crisis – is more likely to be referenced again than a completely separate document. Similarly, an update to the internal crisis management handbook, or an addendum to the disaster recovery procedures are also likely to be looked at again.

A major goal here is to share knowledge with those who were not involved in the crisis experience – possibly years after the actual situation occurred – so that crisis pitfalls and incident response mistakes are not repeated.

Communicating with Regulators, Partners, and the Public

As an organization's cyber crisis develops, there are many communication opportunities and requirements with regulators, partners, the public, or other interested external parties. Communications *opportunities* are those times when an organization can *choose* to communicate and potentially improve its position through constructive, solution-oriented messages. Communications *requirements* are those times when an organization *must* communicate to satisfy regulatory, contractual, or other obligations.

When the crisis situation is grim and a lot is at stake, people will expect an organization to tell them what is going on and what is being done about the situation. Crisis communications need to be carefully crafted, and should consider the following questions:

- *What does the other party need to know?*
- *What does the other party need to do in response to that knowledge?*
- *What is the organization going to do next, now that it has shared information with the other party?*

If an organization is issuing a *public* statement, the statement needs to be crafted in terms of what the public needs to know, what the public needs to do, and what the organization is going to do next. If an organization is issuing a statement to a *regulator*, the statement needs to be crafted in terms of what the regulator needs to know, what the organization thinks the regulator will do, and what the organization is going to do next. Communication statements need

to accurately convey the appropriate facts, guard against sensationalism and misinterpretation of those facts, and communicate what the organization thinks the recipients should do with the information it is sharing with them.

An organization needs to communicate that it understands and appreciates the gravity of the situation. An organization must stress that everyone needs to "do the right thing" to manage the issues involved. Maybe the communications are about confidential information that was leaked, services that are not available, or money that was stolen. An organization should communicate what it knows, that it cares, and that it wants to work constructively with external parties to resolve the situation in a mutually beneficial way.

This section considers some of the topics an organization should consider when managing its eternal communications related to a crisis situation. This includes considering how the organization's communications personnel, legal department, and external experts can work together to craft and manage external messaging. It also includes how an organization may engage with external parties and the public to have constructive dialogues regarding the crisis and its consequences. Finally, this section describes how an organization may provide credit monitoring or other services related to the crisis, and deal with ongoing litigation afterward. These topics are shown in Figure 13.9.

Figure 13.9: Communicating with regulators, partners, and the public involves crafting clear communications to tell stakeholders what they need to know, what they need to do, and what the organization is going to do next.

Engaging Legal and Communications

Organizational public communications will likely need to be reviewed by the legal department. Legal can perform the following activities to support the communications effort:

- Write first drafts of communications.
- Write outlines of the major points to be covered.
- Write "do" and "don't" lists of key points to make and to avoid.
- Review draft messages and suggest changes and edits.

Legal review should include cross-checking communications messages for applicable regulatory considerations, contractual obligations, alignment with messaging from other organizations under similar circumstances, and overall consistency.

Engaging Outside Experts

In a crisis, an organization may want to engage outside experts with experience in managing these types of situations, including external and public messaging. Consultants with experience in handling these types of situations and their own lessons-learned regarding what worked well and did not work well can be valuable and helpful. An organization may also want to model its communications on successful communications from other organizations that have gone through their own breach-related public relations challenges, such as Facebook or Expedia. An organization only has one chance to "make first impressions" regarding its particular situation. If an organization can leverage outside expertise to do that smartly, all the better.

Working with Regulators and Law Enforcement

An organization will likely have to deal with regulators, law enforcement, and other government authorities when dealing with breach-related situations. Interacting with regulators and law enforcement may be at the local, state, national, or international levels, or combinations of all four. The organization's legal department should carefully oversee this interaction. While government authorities' main goal is to serve the public interest, they are usually interested in collaborating with an organization rather than having an adversarial relationship, if possible. An organization should share with them what it can and do its best to be open and truthful as much as possible. When dealing with regulators, it can be helpful to everyone if the organization shares with them (in writing, if possible) its interpretation of what its obligations are under the applicable laws and regulations. If government representatives do not agree with the organization's approach, a written outline can help keep the disagreements focused on the interpretation of the requirements, rather than on disagreements over whether the organization's response is appropriate or not.

Complying with Contractual Obligations and Partner Communications

An organization's other legal obligations tend to center around contractual obligations. These obligations can also include requirements levied upon the organization by compliance standards bodies, like the payment card industry data security standard (PCI-DSS) for credit card processing, or Health Information Trust Alliance (HITRUST)[12] for medical information. These obligations tend to fall into the following two categories:

- Things that an organization is supposed to be doing to *comply* with the requirements of a contract.
- Things that an organization is required to *report* to a standards body, a partner, or the public.

Communications related to these obligations tend to center around explanations of why the organization is or is not complying with the standards (even though something went wrong), or disclosures that are mandatory under the requirements of the standard or contract. It is possible that requirements will include specific parameters to disclose or discuss – some requirements may even include templates for reporting issues – but most likely, it will be up to the organization to decide how much to share and exactly which details to disclose. Organization lawyers will likely be interested in carefully reviewing these potential decisions and the communications that result from the choices involved.

Making Public Disclosures

Public disclosures are the most sensitive communications to draft, as they will be subject to the withering court of public opinion. Historically, the public – and their advocates in the press – does not tend to be sympathetic to organizations that are hacked, suffer a breach, or otherwise have cybersecurity issues. While regulators, standards bodies, and business partners may be understanding of

12 Health Information Trust Alliance (HITRUST) is a company that integrates standards, regulations, frameworks, and organizational requirements into the HITRUST Common Security Framework (CSF). The framework helps to protect data, satisfy compliance requirements, and implement security and privacy controls. Representative CSF source information includes materials from the International Organization for Standardization (ISO), European Union General Data Protection Regulation (GDPR), and U.S. National Institute of Standards and Technology (NIST).

explanations conveying the nuances of what exactly happened and how the organization may not be at fault, public opinion may tend to be more headline-oriented and sensationalist.

An organization needs to carefully consider the sound bites it communicates. The press will look for potential headlines indicating numbers of hacked records, profiles of affected people, and descriptions of possible consequences. The press's interest may fall off quickly after these three details are ascertained. An organization needs to be careful and focus on what is known at the time. If the organization initially announces that a million records *may* have been compromised, and then comes back to state that only a thousand records were *actually* compromised, it will find that the initial "million" estimate will never disappear. The organization probably would have been better off not disclosing the number of breached records in the first place and waiting until the numbers were better understood.

The press dislikes information gaps when reporting the details of a cybersecurity issue. The press may try and fill the gaps with the best estimates it can obtain – either from the organization's website or through speculation from an "expert" consultant. Unfortunately, once the description of the issue gets out into the public, the facts and the messaging about the facts become difficult to control. Misperceptions and miscommunications may never be corrected, once they have been published by the press and consumed by the public.

Communicating via Bidirectional Engagement

As part of an organization's outreach, it may want to engage bidirectionally with the various interested parties. This engagement may involve telephone customer support, e-mail communications, social media like Twitter or Facebook, or customer forums on an organization's website. When dealing with business customers or partners, bidirectional engagement may involve intranet sites, support forums, and chat posts.

There are lots of ways for everyone to engage in the dialogue and communicate. However, there are several challenges with these interactive, bidirectional engagements. With multiple organization representatives engaging in communications via telephone, e-mail, chat, and face-to-face, there are many opportunities for messages to become distorted, diluted, or confused. Regardless of what organization personnel think they communicated, the people receiving the communications on the other side may interpret things in their own ways, often in ways completely different from the message that was intended. Throw

in some culture and language gaps, as well as people posting to social media to further their own goals, and communications can go sideways quickly.

When engaging in bidirectional communications, organization personnel should have clear guidelines on what they are to share and what they are not to share. An organization should make clear what is "on the script" for public dissemination, as opposed to internal communications which may contain proprietary details. An organization should make it clear how personnel are to respond when a customer asks them a question to which they may know the answer but are not supposed to share.

Providing Credit and Identity Protection

As a part of a crisis response, an organization may need to provide credit monitoring, identity theft, or other protection services to its customers or partners' customers. The good news is that these services are available at economical prices from providers like Equifax,[13] and can be effective at guarding against identity theft once protections are put into place. The bad news is that the costs for these services, multiplied by millions of customers over multiple years, can become significant.

An organization will want to work with its legal team and consultants to pick protection levels that are reasonable for those affected customers while keeping consistent with industry norms. Unfortunately, customers who are already leery of online services may be even more put off when they realize that their "free" identity theft service requires them to set up yet another online account username and password. In addition, if the cyber incident involved stolen credit card numbers or bank account information, an organization may find its banking or card service providers also charging it for account remediation or replacement credit card services.

Understanding Post-Crisis Litigation

There is the possibility of litigation after the cyber incident. This possibility can occur in almost any type of cyber incident, regardless of the actual damages that occurred, if any. Precedents on legal liability for cyber incidents are still

13 Equifax, Experian, and TransUnion are the three largest consumer credit reporting agencies.

being established, and many important cases have ultimately been settled out of court with no admissions of actual wrongdoing. Depending on the specifics of the cyber incident, the threat of litigation may be relatively short-lived, or it may go on for years after the incident has been otherwise resolved.

Potential litigation costs may affect an organization's balance sheet, stock price, investor choices, and partner relationships for years, particularly if legal issues are not swiftly resolved. Should an organization find itself in the midst of a class-action lawsuit, it should seek legal counsel with experience in these types of cases and work closely with counsel on its strategy. In these types of cases, it is important to understand the laws and regulations affecting the organization's liability, the potential sources of damage for the victims, and the limits on the compensation the organization may become obligated to pay. Finally, an organization and its legal team should consider the pros and cons of obtaining swift legal resolution, versus spending months or years in court trying to get the best possible financial settlement.

Cyber Insurance

In risk management, people control the problems that they can, and for the things they can't control, they insure. Cyber insurance is business insurance designed to help reduce the costs of dealing with a cyber incident. Cyber insurance may help to cover costs related to hacking, theft, fraud, business interruption, ransomware, and customer data compromise, breach, or loss. It may cover the costs of cyber incident investigations and forensics, and may even include coverage for extortion and damage to an organization's reputation.

Over the past three decades, the cyber insurance industry has grown from a minor industry in the 1990s to a multi-billion-dollar industry today. In the face of continuing threats and cyber damages to organizations, cyber insurance has become a must-have for many organizations. Although it is an important and growing industry, cyber insurance has its own sets of challenges. The industry is still quite small and centered around a small group of insurance companies actively underwriting policies. The actuarial data for cyber insurance is still immature, so insurance companies have a hard time pricing policies and understanding what risk factors should drive policy pricing. Everyone continues to struggle with how to measure and reduce cyber risk – and thus policy premiums – for organizations seeking cyber insurance. Cyber standards are still relatively immature, vary widely across industries, are constantly evolving, and are difficult to assess. It's not as if an organization can simply take a test or complete a checklist and understand its risk of being hacked.

Finally, many of the worst hacks of the past decade have been perpetuated by nation-state attackers. In many cases, insurance companies have argued that these types of attacks are excluded from coverage under "wartime exclusion clauses," even though there are no troops on the ground, no front lines, and certainly no shooting.

We are engaged in a Cyber Cold War that does not show any signs of ending.

This section considers some of the topics an organization should consider regarding cyber insurance and how it may be able to cover some of the costs related to an organization's cyber incident or crisis situation. This includes describing organizational cyber insurance policies, common cyber policy limitations, and wartime exclusion issues. It also includes considering how an organization might utilize its cyber insurance policy in terms of opening a claim and tracking identified costs covered by that claim. Finally, it includes considering how an organization's insurance may seek to reduce its cyber risk through compliance requirements and audits. These topics are shown in Figure 13.10.

Figure 13.10: Cyber insurance involves understanding how insurance policies work, the limitations of cyber insurance, and the requirements that may come from working with insurance companies to manage cyber risks.

Cyber Insurance Policies

While cyber insurance is its own insurance category alongside liability, accidents, or crime protections, there are also multiple subcategories of cyber insurance. These subcategories may be coverages within a single cyber insurance policy, or they may be separate policies with their own rates and contracts. Cyber insurance subcategories may include coverage for the following types of costs or damages:

- Cyber incident investigations
- Forensics and interactions with law enforcement

- Operational costs related to business impacts of damaged computer systems
- Other damages caused by hacking
- Reputational impacts
- Bank and credit card fraud
- Credit monitoring and other customer restitution
- Payment of cyber ransoms or extortion
- Restoration and rebuilding of damaged computer systems

An organization should carefully review its cyber insurance policy and check its definitions. What an organization calls "hacking" may not be the same as what the insurance company calls "hacking." Or worse, important terms may not be defined at all, leaving definitions up to interpretation or negotiation when there is a claim and real money is on the line.

An organization also needs to understand how an "incident" is defined for the purpose of filing an insurance claim. This understanding is important because it may be days, weeks, or months after the actual hacking occurred before an organization finds the resulting issues in its IT systems. An organization needs to be able to identify incidents after the fact, do the appropriate accounting, and then get compensation in accordance with the coverage of the insurance policy.

Policy Limitations

Cyber insurance is a relatively young industry and everyone is still figuring out what works and what does not. An organization's policy may have separate terms, exclusions, and other coverage limitations associated with each subcategory, so the organization needs to carefully review cyber policies. Just as a home insurance policy may only include limited coverage for computers or jewelry, a cyber insurance policy may include only limited coverage for specific cyber scenarios or types of cyber damages.

A cyber policy may also include a significant deductible, which is designed to limit potentially frivolous claims. An organization also needs to carefully look for clauses that might trigger exclusion from coverage. If coverage is excluded in the case of "mistakes" on the part of an organization's personnel, then its ability to make claims may end up being limited. In reality, complex IT systems tend to be riddled with "mistakes," oversights, and minor glitches. Arguing that the IT systems were properly maintained may be difficult, in the midst of a claim.

An organization should also carefully review policy time limitations. An organization needs to make sure that insurance coverage is coordinated with its ability to detect and investigate incidents. For example, an organization does not want its coverage to be limited to the preceding 30 days when most cyber incidents are not detected until months after the fact.

Wartime Exclusions

Cyber insurance may have a wartime exclusion clause. While such a clause makes perfect sense in the case of physical damages – it's pretty clear when a tank drives through your front yard – they cause tremendous confusion for cyber damages. First, there is an attribution problem. It is difficult or even impossible to conclusively prove who the hackers are or where they originate. Second, there is a tool re-use problem. Just because the U.S. National Security Agency (NSA) used a tool in the past does not mean they are the ones using it now against an organization. For example, the NSA developed the devastating "EternalBlue" hacking toolkit that criminals and nation-state hackers subsequently adapted for their own use around the world.

Cyber insurance coverage should define how and when the wartime exclusion clause would be invoked. The cyber policy should clearly address situations where the facts may be incomplete or unclear, or where attribution is not possible. An organization does not want such uncertainty working against it, nor does it not want to have the onus on it to "prove" the identity of those who attacked it.

Covered Cyber Costs

When an organization does place a claim, it will provide the insurance company with an accounting of the damages and costs associated with the incident. The cyber policy coverage may allow for estimation of costs or may even provide a schedule of compensation, such as $1,000 for every computer to be reimaged. However, an organization needs to be careful of such fixed schedules. An organization should ask questions such as the following:

- *Does the cyber policy allow for cloud services, virtualized systems, or software as a service (SaaS)?*
- *Does the cyber policy include coverage for external service providers, rental of temporary equipment, engagement of cloud services, or other ancillary costs?*

Another possible compensation approach is for an organization to track the costs of hardware, software, labor, and services associated with the incident, and then get reimbursement for those costs, minus the deductible. This approach is much more flexible, but requires that an organization has good accounting of its costs. *Can an organization identify which hours were related to the incident versus those hours involved in "keeping the lights on" and other business tasks?*

If an organization uses a timekeeping system, such accounting can be made significantly easier by creating a charge number for the incident and its costs. However, this accounting only works well if an organization can quickly create charge numbers for the incident, and then direct its staff to use them – probably not an organization's top priority when dealing with a crisis situation.

Finally, an organization's insurer will want a time period to limit the costs associated with the claim. An organization's cyber crisis will likely end at different times for different departments. An organization's accounting of the crisis costs will need to be coordinated with those events, and may then be subject to further limitations under its cyber insurance policy.

Compliance Requirements

The cyber insurance company will likely place requirements on how an organization performs cybersecurity to reduce an organization's risk and the insurer's risk of payout. In the 2000s, insurers used cyber requirement checklists to confirm that an organization met a minimum set of requirements. For example, an organization needed to have a firewall on its network and use antivirus software. Over time, these checklists have evolved and become more comprehensive. Today, such checklists are likely to require security protections for an organization's endpoints, servers, devices, networks, accounts, and cloud services.

For example, an insurer may require an organization to assess its cybersecurity against established security frameworks such as those from PCI-DSS, HIPAA, HITRUST, SANS, NIST, ISACA, or SSAE-18.[14] A cyber insurer may require that an organization get a framework assessment performed by a third-party assessor or auditor. Such activities may drive up an organization's costs and compliance complexity. Where possible, an organization should try to coordinate its insurance

14 Payment Card Industry Data Security Standard (PCI-DSS); Health Insurance Portability and Accountability Act (HIPAA); Health Information Trust Alliance (HITRUST); SysAdmin, Audit, Network and Security (SANS); National Institute of Standards and Technology (NIST); Information Systems Audit and Control Association (ISACA); Statement on Standards for Attestation Engagements No. 18 (SSAE-18, formerly SSAE-16, and before that, SAS-70).

requirements with its compliance requirements so that the same assessment or audit can be used to satisfy the needs of its insurers, regulators, and business partners.

Resilience

Things can go wrong, and go wrong big-time, when a cyber crisis occurs. Cleaning up malware on a single computer – or even a couple of computers – is a straightforward task. However, countering an active, experienced adversary who has control of an organization's infrastructure and its IT environment is non-trivial and bone-chilling – the organization's business may be at stake.

Engaging with a cyber adversary can be like *cyber hand-to-hand combat*.

While it is both possible and likely that an organization will eventually wrestle back control of its IT enterprise from the attackers, the chances are good that there will be collateral damage – perhaps a lot.

Automated cyberattacks can take out hundreds or even thousands of computers per hour, and scripted attacks can occur far faster than humans can respond. Attackers may perform a "scorched earth" attack on an organization's IT environment on their way in, on their way out, or long after they are gone, just to distract the organization from what really occurred. In the case of ransomware, the damage may be an integral component of the attack. Ransomware cyberattackers hope that an organization will choose the less painful route of paying the ransom rather than going through the pain of rebuilding everything. To counter these potential challenges, an organization's best defense should include preparation, vigilance, and resilience, as follows:

- *Preparation* involves being ready for the things that may go wrong and having a plan to respond quickly when an organization detects a deliberate attack.
- *Vigilance* involves having visibility within an organization's IT environment, monitoring cyber activity with its sensors, and then responding when alarms are triggered by potential cyberattacks.
- *Resilience* involves having robust IT systems that can continue to function even when degraded by cyberattacks (or corresponding response activities) and can be rebuilt quickly when required.

By being prepared, vigilant, and resilient, an organization can prevent, detect, respond, and recover quickly from whatever attackers may throw at it. At a high level, resilience involves:

- Separating the knowledge for recovering an organization's IT systems from the actual process of doing the work to recover those systems.
- Having redundant and excess capacity, so that critical business services can continue to be delivered during adverse circumstances, and can be restored quickly when needed.

Robust resilience will not be achieved if an organization relies on people to rebuild things one computer at a time, one application at a time, all manually and by hand. An organization needs to capture the knowledge of how to rebuild those computers, applications, accounts, services, networks, and containers, and have that knowledge standing by for when the organization needs it – already in the machines and available to the organization as fast as the machines can work.

Robust resilience is not about notes, procedures, or recordings – it is about automated scripts. Only by scripting an IT environment – and everything in it – will an organization be able to achieve the resilience needed and the ability to rebuild its environment as quickly as an attacker can take it out.

This section considers some of the topics an organization should consider related to resilience for its IT systems and cyberdefenses. This includes describing how an organization can prepare its IT environment to be resilient, and the techniques it can use to achieve resilience using available technologies. This also includes describing how a resilient foundation may lead the organization toward "next-generation" cyberdefenses at some point in the future. These topics are shown in Figure 13.11.

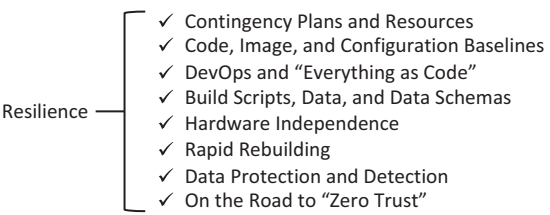


Figure 13.11: Resilience involves taking steps to make the organization's IT environments and cyberdefenses resistant to advanced cyberattacks, and able to rapidly recover under a wide range of circumstances.

Contingency Plans and Resources

Resilience starts with planning. An organization should think through what capabilities it needs to be resilient. It likely will not be able to engineer everything for resilience, but planning exercises can be helpful to identify critical systems,

single points of failures, and complex interdependencies. Disaster recovery exercises may be helpful in defining and refining these plans over time. As a part of this planning effort, an organization will likely identify resources that would be helpful for a variety of rebuilding scenarios. These resources may include offline backups, alternate systems or service providers, and excess capacity in production systems. One common technique is for development/quality assurance (QA) environments to be able to be repurposed for production. This technique is a useful dual-use approach that makes these resources useful during normal operations, but makes them also available to support the organization in an emergency. They just need to be isolated enough that a production attack will not take them out too.

Code, Image, and Configuration Baselines

Once an organization has the resources it needs to support resilient computing, it needs to have configuration control so that it can rebuild things in a hurry. Configuration control should include custom code, software images, and system configurations. While configuration management databases (CMDBs) tend to be good starts toward having this information, they seldom contain enough detail to permit complete rebuilding on their own. Ideally, code, software, and configurations should all be linked together so that a single "build" or "make" command can trigger the reconstruction of entire systems onto any target computing infrastructure.

DevOps and "Everything as Code"

Cloud computing takes this configuration methodology to its logical conclusion, in the form of Development Operations, or DevOps. In DevOps, the entire configuration of a computer, application, system, or network can be represented using configuration code or scripts. The exact language depends on the cloud platform and the development tools being used to control the platform. However, the DevOps concept is consistent and includes major public clouds like Amazon, Microsoft, and Google, as well as private clouds using technology from VMWare, Nutanix, and others.

In DevOps, a server computer's configuration might be represented by a JavaScript Object Notation (JSON) script that describes all of the build parameters for the server – including the installation of software onto the server – and the running of that software once everything is installed. A complex application

might be composed of a set of scripts to configure the individual servers, application code, supporting databases, network interfaces, load balancers, and security features. These components – each represented by their own sets of configuration scripts – might then be connected together hierarchically. In the complete hierarchy, services, applications, computers, and multi-computer systems would all be represented and configured through such automated scripts.

Taken to its logical conclusion, an organization's entire data center might be represented through this complex hierarchy of scripts, and could be rebuilt automatically just by rerunning the configuration script hierarchy. In short, DevOps can enable an organization to "store everything as code."

Build Scripts, Data, and Data Schemas

Once everything is represented as code, an organization's IT environment ends up divided into two components. The first IT environment component is the configurations and interconnections of the individual IT components, software applications, and tools. These configurations and interconnections are represented by the *build scripts* an organization maintains under an organization's "everything as code" cloud methodology. Rather than change individual systems, organizational developers would update the configuration scripts, and then rebuild the systems to the new specifications. Not only are the systems changed, but the configuration baselines are also simultaneously updated at the same time.

The second IT environment component is the *data* that runs on those systems and the *schema* that data adheres to. The data must be kept separate from the systems that manipulate it so that the systems can be reconfigured and rebuilt while leaving the data intact. Easy ways to do this separation are to put systems and data on separate infrastructures, store the data in cloud database services like Amazon's Simple Storage Service (S3), or keep the data on separate virtual drives within an organization's computing environment.

The *data schema* is the "contract" between the data and the systems manipulating the data. Changes to systems that do not affect the schema can be performed without too much concern. However, changes that affect the data schema must be carefully coordinated. Systems containing application code written for a new data schema cannot directly use data formatted in an old data schema, and vice versa. Updates that affect the schemas require careful orchestration to avoid system conflicts and possible data corruption. Fortunately, data schemas do not tend to change anywhere near as often as the data itself – nor does the application logic being applied to the data – so in practice, this separation does not tend to cause major problems.

Hardware Independence

Once an organization has DevOps and data separation in place, it will be positioned to make its entire application, service, or even computing environment hardware independent. With hardware independence, IT services can be deployed to any computing environment anywhere, provided that sufficient central processing unit (CPU), random access memory (RAM), and storage resources are available and the scripting environment is compatible with what an organization has already prepared. With hardware independence, an organization can point its build scripts to a different data center, a backup location, or a public cloud, and then rebuild everything just the way it was built in the original instantiation. Only minor changes should be needed to adapt to the particulars of the specific target computing environment.

This hardware independence also means that an organization's IT environment will not be tied to the hardware particulars of Dell, Hewlett-Packard (HP), International Business Machines (IBM), or other computing hardware manufacturers. An organization will be able to be hardware independent and hardware agnostic, treating the computing environment as nothing more than raw hardware capacity available for the use of its applications and services.

Rapid Rebuilding

With DevOps, data isolation, and hardware independence, an organization will be able to take its resilience to the next level and achieve rapid rebuilding. Rapid rebuilding means that the limiting factor for restoring operational capability is simply network and computing speeds. Little to no time is spent waiting for people.

For example, an organization's primary cloud provider suffers an outage and becomes unavailable. However, the organization has backup copies of its operational data – perhaps stored at a secondary cloud provider – along with a copy of its offline build scripts and data schema specifications. Armed with those two sets of information, the organization can then go to an alternate cloud provider, rebuild its operational systems, and then connect the rebuilt systems to the backup copy of the operational data.

As long as the data and the applications are using the correct data schema, everything should work and the organization should be able to quickly restore its services. Rather than taking days or weeks to rebuild, the process only takes minutes or hours. In this way, rapid rebuilding using DevOps can be more than *100 times faster* than manually reconfiguring systems and restoring data from backups. This can be a game-changer.

Data Protection and Detection

Another bonus of having a strict separation of production data from applications and services is the possibility of building specific protections integrated into the data subsystem itself. When data is consolidated and managed strictly as data, an organization can focus its protections on the data itself rather than on the applications hosting or handling the data.

For example, an organization can build strict access controls around the data so that it is only directly accessible by the applications, backup services, and authorized administrators. To accomplish building strict access controls, an organization can perform the following activities:

- Implement advanced data protection mechanisms, such as complex cryptography, directly into the data structures and the data storage subsystem.
- Implement a strict audit trail that captures all data accesses, regardless of their origins, and then do alerts based on the analysis of that audit trail.
- Perform analytics directly against the data elements to potentially detect common attack patterns such as database dumps, walks, or deletions.
- Leverage emerging data protection capabilities such as quantum-safe cryptography or blockchain without having to change the applications relying upon the data.

So long as the data schema and application programming interface (API) remain the same, the applications will continue to operate normally, even though organizational data protections are improving.

On the Road to "Zero Trust"

All of these capabilities can be integral steps on the road toward next-generation cyberdefenses, resilience, and "zero trust." Zero trust has become a popular buzzword, embraced by many cybersecurity vendors in the context of their specific niches and capabilities. So-called zero trust solutions are available from popular cybersecurity vendors for networking, computing, applications, and IoT devices, to name a few.

Looking at zero trust from a different perspective, it can mean that every component of an organization's IT environment is compartmentalized, isolated, and managed, with strict control of what gets deployed and what operates within the IT environment. From this perspective, only trusted code from trusted users in a trusted environment is permitted to communicate across the trusted network

to perform trusted transactions. All activities are authenticated, authorized, validated, and journaled so that they can be analyzed for correctness and rolled back if necessary. This zero trust vision is the access-controlled, DevOps-deployed, cloud-based, dynamic, responsive, and resilient organizational IT environment of the future.

Chapter 14
Looking to the Future

While the cyberattack of the day may feel like we are in a perpetual "groundhog day" loop of "vulnerability," "patch," and "repeat," the fact is that IT and cybersecurity have evolved a great deal over the past decade. Most likely, they will both continue to evolve over the decade yet to come. This evolution includes a number of factors regarding how business IT is performed, and how cyberattack threats will attempt to exploit business IT to benefit the cyberattackers. Attacker motivations of the past are not going to change in the future. Crime will remain crime, espionage will remain espionage, and thrill-seeking and terrorism will most likely continue as they have in the past. Keeping pace with threat actors and their latest techniques is an ongoing security challenge.

What most likely *will* change is the scale, speed, and style of cyberattacks in the future, as IT becomes even more pervasive, more powerful, and more complex. The cloud will enable even modest businesses to harness the services of thousands or even millions of computers, while future IT services will make advanced technologies like machine learning and artificial intelligence available to everyone. This concentration of data and computing power will in turn lead to new vulnerabilities, new exploits, and new attacks. "Scorched earth" cyberattack techniques will wipe out whole data centers (or at least hold them hostage), along with the data and business value trapped within them. Resilience and the ability to absorb cyberattacks will take on a new importance in IT planning.

As always, the people factor will remain a constant, including the tension between the business people trying to conduct the organization's business and the security people trying to protect it from harm. The organization's first line of vulnerability, as well as its first line of defense, will continue to be its people. The most successful security professionals will be those who understand the power of collaborating to find "win-win" security relationships and opportunities.

This chapter describes some *evolving IT trends* and how they are going to interact with *evolving cyber threats*. It describes how the successful cyber professional can use an awareness of evolving IT trends and cyber threats to *stay calm, aware, and prepared* for future attacks while maintaining the balance between the priorities of the organization's cyber protection and its business needs. This chapter closes with a few recommendations for cybersecurity professionals about how to *be cautious but smart* as they attempt to balance these competing priorities.

https://doi.org/10.1515/9781501506529-014

Evolving IT Trends

Perhaps the greatest transformation of IT over the past decade has been the rise of cloud computing. People can harness the power of hundreds, thousands, or even millions of computers without caring about where they are geographically located, how they are configured, or what hardware they are using. Technology has come a long way from when servers were built one at a time – each server was a little bit different, and most servers were running at a fraction of their actual computing capacity.

On the other hand, another trend everyone can see quite clearly is millions of people with little supercomputers in their pockets, masquerading as phones. This trend is visible because people are so busy looking at their phones that they may not see much else. Along with the trends in cloud and mobile computing is the explosion in internet-connected devices on work and home networks. When all three of these trends are combined, massive concentrations of data, along with correlating analytics, enable machine learning and artificial intelligence algorithms to find previously unseen connections and patterns.

This section describes some evolving IT trends and how these trends affect the ways people interact with IT systems and capabilities, as shown in Figure 14.1.

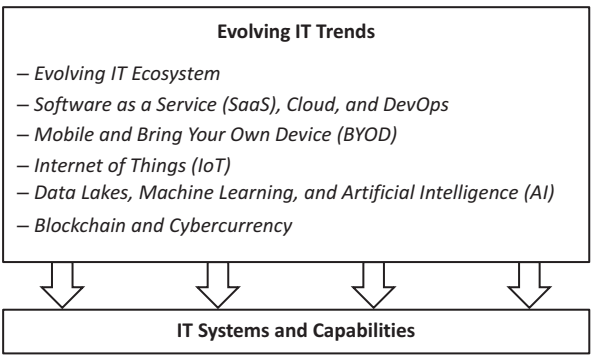


Figure 14.1: Evolving IT trends include the rise of cloud computing, mobile devices, network-connected equipment, and advanced data capabilities in the future.

Evolving IT Ecosystem

When looking at the evolving ecosystem of IT systems surrounding us, we see changes that have occurred over the past decade and will no doubt continue

into the next decade. More capabilities are being fueled by software running on cheaper, more powerful, and more prevalent hardware platforms. *Who would have predicted a full-blown computer for $50?*[1] Such a computer may not be extremely fast or powerful, but it does not have to be to power a sensor, perform some analysis, or upload data to an internet server. This evolving IT ecosystem is coming from an increasingly complex supply chain providing devices, applications, analytics, and services. That supply chain is, in turn, connected to our devices and IT systems in myriad ways.

Software as a Service (SaaS), Cloud, and DevOps

One of the most prominent examples of supply chain evolution involves the rise of cloud computing. By using software services from third parties, organizations can outsource common business processes – like payroll, sales tracking, collaboration, and cybersecurity – to organizations that specialize in them and can deliver better results for lower costs. By using cloud computing, organizations can avoid huge investments in data centers and servers while achieving much greater flexibility in sizing and scaling their IT systems to meet demand. By using DevOps software development methodologies, organizations can dramatically reduce their time-to-market and increase their agility in fixing bugs, developing new features, and responding to customer requests.

Mobile and Bring Your Own Device (BYOD)

Few can deny the impact mobile computing has on our lives. What is perhaps even more interesting to observe is how it is starting to impact business. Flight attendants are able to run their flight services – checking in passengers, confirming manifests, processing credit card purchases, and looking up procedure checklists – all from a single device. Medical staff are able to track their patients on a single tablet without having to touch a piece of paper or go back to a nurse's station. Contractors are able to do estimates, quotations, invoices, and billing, all while standing in front of the customer and without having to call in or go back to the office. Through BYOD policies, organizations can deliver much of their

1 The Raspberry Pi project delivers a bare-bones personal computer for less than $50; the Raspberry Pi 4 can even run a Linux desktop operating system with web browser and office software.

capabilities to employees and contractors on personal devices while still keeping the organization's sensitive data protected and access-controlled.

Internet of Things (IoT)

Similar to the rise of mobile devices is the explosion in the number of network-connected "smart" devices. These devices can range from doorbells and security cameras, to refrigerators and televisions, to remote wearable heart monitors and other specialized sensors. In the workplace, smart devices can include telephones, printers, controllers, and conveyer belts, not to mention entire cars and trucks. These devices can upload data to the cloud, download data from the cloud, perform their own processing, or enable people to check their e-mail and social media from every room in their homes or offices.

Data Lakes, Machine Learning, and Artificial Intelligence (AI)

On the infrastructure side, "data lakes" enable the collection of huge, petabyte-scale data sets, and new analytics tools can query and analyze those data sets in entirely new ways. These huge data sets are then fueling new capabilities in machine learning and artificial intelligence. While still in its infancy, techniques coupling massive data sets with graphics process unit (GPU)-powered supercomputing are turning what was science fiction a decade ago into artificial intelligence applications today. Such capabilities are yielding impressive results, including facial recognition, intuitive voice assistants, and self-driving vehicles.

Blockchain and Cybercurrency

A discussion of the future of computing would not be complete without mentioning blockchain. The U.S. National Institute of Standards and Technology defines blockchain as follows:

> tamper evident and tamper resistant digital ledgers implemented in a distributed fashion (i.e., without a central repository) and usually without a central authority (i.e., a bank, company or government). At their basic level, they enable a community of users to record transactions in a shared ledger within that community, such that under normal operation of the blockchain network no traction can be changed once published.

> [T]he technology is called blockchain because the transactions are grouped and published separately in distinct data structures called blocks, which are cryptographically linked together and distributed in a peer-to-peer network to prevent tampering of previously published transactions.[2]

This elegant solution to a problem of mutual online trust makes it well-suited for cybercurrencies (such as Ethereum, Factom, MaidSafe, Bitcoin, and Ripple) that have become a new asset class for users and investors alike. Researchers are considering how blockchain technology might be leveraged for other applications such as "smart contracts," banking, healthcare, manufacturing, regulation, or supply chain management.

Evolving Cyber Threats

As IT continues to evolve, transform, and spread throughout our lives, vulnerabilities within IT and cyberattacks to exploit those vulnerabilities will most likely continue. It is naive to think that future devices, operating systems, and applications will be less vulnerable to bugs, glitches, or hacks. While everyone will continue to strive for good-quality software systems free of devastating bugs, the sheer complexity of IT systems means that certain amounts of vulnerability and exploitation are going to be inevitable. Therefore, cyberattackers are still going to be able to do their thing – targeting our accounts, computers, applications, and servers – to achieve their goals.

What is going to change is the complexity, velocity, and danger of cyberattacks in the future. Consider the following potential scenarios:

- When a home has 100 network-connected devices (or an organization has 10 of them per employee), the odds that one or more of those devices is compromised and malicious are much greater than when there were only a couple of connected devices.
- When an organization has relationships with dozens of external organizations all handling the same databases of proprietary organizational data, the risk to those databases increases considerably.
- When malware can spread across an organization's IT environment as fast as the computers can operate, defenders may have only seconds to detect and respond to the malware before it is too late.

---

2 Dylan Yaga, Peter Mell, Nik Roby, Karen Scarfone, "Blockchain Technology Overview," National Institute of Standards and Technology, Gaithersburg, MD, NIST Internal Report 8202 (NISTIR 8202). https://doi.org/10.6028/NIST.IR.8202.

– When cyberattacked devices are controlling lights, doors, cameras, machines, or vehicles, the potential damage can include physical property and personnel safety, in addition to damaging data or software.

This section describes how evolving IT trends lead to new generations of cyber threats targeting data, applications, IT systems, equipment, and people. These threats can affect stakeholders including organization employees, customers, partners, service providers, vendors, and guests. These evolving cyber threats are illustrated in Figure 14.2.

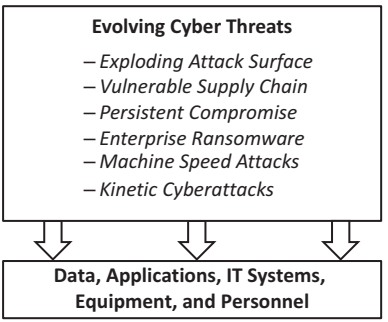


Figure 14.2: Evolving cyber threats may pose new dangers to data, applications, IT systems, equipment, and people.

Exploding Attack Surface

With the proliferation of network-connected devices in the office, in the plant, and at home, the exploitability of these networks is higher than ever. At the same time, the use of mobile computing, smartphones, and tablets continues to increase. While personal computers have generally become more secure over time, the amount of computing capacity and data on those devices has exploded, increasing the danger from even a single compromised system. For connected devices in particular, infrequent software updates mean many of these devices become vulnerable over time, and those vulnerabilities are never actually remediated. In addition, the embedded computers that run smart devices – think IoT – are often completely undefended. Security protection is often left up to the individual to implement. When this security does not get implemented, the unsecured devices offer cyberattackers easy targets to access their victims' IT environments.

Vulnerable Supply Chain

At the same time, expanding business relationships mean that an increasing number of partners are directly linked into organization IT systems, databases, and applications on an ongoing basis. These connections may include the following potential scenarios:

- Remote software developers writing code for applications within the organization's data center or IT services.
- Remote data processors connecting to databases, performing analysis, and then injecting results back into those same databases, or into other third parties' back-end systems.
- Direct network connections enabling multiple application servers to connect to third-party back-end servers or cloud services, and vice versa.
- Contractor personnel connecting to organizational networks to support customers, deliver on business partnerships, or provide other needed services.
- Remote connections from equipment manufacturers that enable them to monitor, troubleshoot, and maintain their products installed in hospitals, factory floors, or machinery plants.
- Interconnections among cloud services to enable human resources, enterprise resource planning, financial, and other organization critical services to interoperate, while also creating a complex web of trust among the organization and its service providers.

In these scenarios, it may be possible for cyberattacks that succeed against one organization in the supply chain – or one person in an organization – to then move laterally and target the partner organization as well. As supply chain relationships become more complex, this trend will likely become more common and more troublesome.

Persistent Compromise

The combination of an expanding attack surface combined with supply chain connectivity means that many organizations may find themselves in a state of "persistent compromise." In this situation, vulnerabilities are always present, exploits and malware are always being injected, and some level of cyberattack is taking place on an ongoing basis. While not ideal, it can be possible to operate in this situation, provided that there are compensating controls and an active cyberdefense to limit the damage. The goal of an active cyberdefense is to catch and repel these ongoing attacks before they can do significant harm.

Enterprise Ransomware

Another concerning trend is the emergence of enterprise ransomware, where attackers target an entire organization's network, take control of it, and unleash ransomware on large numbers of computers and servers, at high speed. These attacks have shown themselves to be effective at taking out hospitals, manufacturers, and even entire municipalities. In some cases, it has taken weeks for computers to be recovered and services restored. In other cases, organizations have ended up paying the ransom rather than suffer an extended outage. Even after paying the ransom, some of these victims have been unable to decrypt their data successfully and have had to rebuild, anyway. The ongoing specter of attacks like these means that organizations must place a new emphasis on detection, rapid response, and recovery.

Machine Speed Attacks

Attacks like enterprise ransomware are only the beginning of a possibly more concerning trend: high-speed attacks that occur at machine speed. In theory, a machine speed attack can progress as fast as the computers operate, going from that first click on a link or an attachment to complete enterprise control, all in a matter of minutes or even seconds. Once cyberattackers have control, these attacks may be just as swift in achieving objectives such as changing data, destroying data, exfiltrating records, or deploying ransomware. In theory, a machine speed attack could perform all of these steps automatically and as fast as the computers, devices, and network will allow. Such an attack will likely proceed unopposed, while overwhelmed defenders stand by, powerless to stop it.

Kinetic Cyberattacks

All of these cyber threats combined lead to a new type of cyberattack that can impact the real world, physical objects, and safety. Such attacks are often referred to as "kinetic cyberattacks." These attacks might unlock a door, turn off a camera, or even disable a piece of lifesaving equipment. At the extreme, kinetic cyberattacks might cause a car to crash, knock out the power, or cause

a factory blast furnace to literally melt down. Consider the following examples of real-world kinetic cyberattacks that have occurred recently:[3]

- A demonstration of a remote hack of a Jeep vehicle where the hackers "were able to cut the car's brakes, shut down the engine, and take control of the steering wheel."
- A tram system was compromised and "four cars were derailed, injuring twelve people."
- A power distribution company was successfully hacked, "ultimately knocking some thirty substations offline."

As physical systems become more connected and dependent on networked computing, kinetic cyberattacks will likely increase in frequency, and potentially in impact as well. Frighteningly, kinetic cyberattacks that cause injuries or deaths may be right around the corner.

Stay Calm, Aware, and Prepared

Knowing that advanced cyberattacks are coming, what are organization IT and cybersecurity professionals supposed to do? Well, they can't just unplug and hide, nor can they stop the organization from continuing to automate. The benefits of connectivity, computing, data sharing, analytics, and artificial intelligence are simply too great to give up. Organizations will continue to invest in next-generation IT capabilities while they continue to struggle protecting the IT capabilities they already have. To keep up, cybersecurity capabilities must evolve concurrent with the organization's other IT capabilities, so that the latest innovations can be protected at the same time they are deployed.

How can cybersecurity keep pace with evolving organization capabilities? First, it is critical to understand that cybersecurity is not a stagnant discipline. The tools and techniques that worked well ten years ago may not work so well today. Furthermore, the tools and techniques that work well today may not be adequate tomorrow. Organizations need to focus on fundamental security factors that are universal and aren't going to change (much) while everything else is evolving. Such factors include security mentality, security responsibilities, and security techniques. These factors will help organizations function success-

3 CyberVista, "Let's Get Physical: How Kinetic Cyber Attacks Can Crush Your Company," August 18, 2018 (https://www.cybervista.net/kinetic-cyber-attacks/).

fully, balance their business and security priorities, and implement "good" security practices. Cybersecurity must evolve as technology continues transforming the organizations it is seeking to protect.

This section describes some cyberdefense truths that will remain true even while cyberattacks, cyberdefenses, and IT technologies evolve, as shown in Figure 14.3.

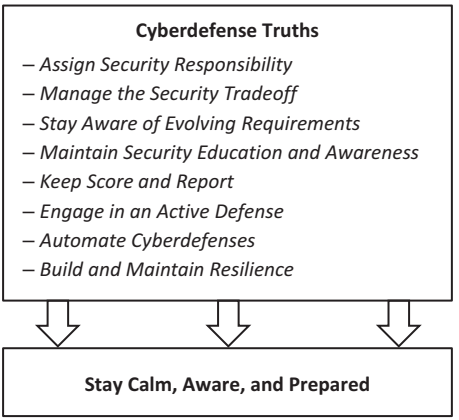


Figure 14.3: Cyberdefense truths will remain constant even as IT and cyberattacks evolve, and can provide a path for organizations to stay calm, aware, and prepared for the future.

Assign Security Responsibility

First off, someone has to be responsible for security, and someone has to champion the cause of security for the organization. This position is frequently in opposition to the rest of the organization, so having a person and a team or department charged with the mission of security is not only important, it is indispensable. Otherwise, cybersecurity will likely get pushed aside in favor of other priorities that are more urgent, more convenient, or more lucrative. The "here and now" of day-to-day operational concerns often take precedence over longer-term cybersecurity planning and strategy development. People may not pay attention to the need for long-term cybersecurity planning unless a crisis situation occurs. Simply stated, effective cybersecurity preparation takes time and teamwork, and an emergency is the wrong time to realize that it has been lacking.

Manage the Security Tradeoff

Security cannot be successful if it is strictly the department of "No." Instead, cybersecurity needs to be the department of "Yes, and . . ." where the "and" is followed by steps the organization can take to conduct itself more securely, avoid dangerous mistakes, and reduce its risk. Security leaders need to frame security considerations in terms the organization understands, like risks to revenue, people, facilities, safety, or reputation. Security leaders need to establish clear guidelines for what "good enough" security looks like, with the understanding that "good enough" is going to be far from "perfect." Executive leaders need to understand there is no "perfect" cybersecurity solution. While perfect security may be desirable, it usually isn't possible, nor does it tend to be very cost-effective.

All organization levels need to understand that intelligent cyberattackers will eventually defeat the organization's cyberdefense measures. It is necessary to design defenses to detect initial incursions, particularly internet-facing systems such as web servers or user endpoints. Defenses need to be layered to contain attacks and delay attackers long enough for defenders to respond. Active defenses need to monitor IT systems, diagnose attacks, and repel attacks before the attackers can defeat the organization's defenses and achieve their objectives.

Stay Aware of Evolving Requirements

Security leaders need to stay aware of what security is required by regulators, business standards, or customer contracts. These requirements may be quite onerous – think banks, hospitals, and defense contractors – and will most likely change over time. Regulations and standards are constantly being updated to handle new technologies like mobile and cloud, new approaches like zero trust, and new threats like ransomware. Organizations must stay abreast of these requirements, ensure they meet the requirements that apply to them, and be prepared to adjust their security as the requirements evolve.

Maintain Security Education and Awareness

When security requirements are known, one of the worst things an organization can do is to ignore those requirements. Organization cybersecurity is a team sport – individuals don't have to do it alone! By educating the rest of the

organization on what its security obligations are and making people aware of how those obligations impact them, others are empowered to assist the organization in its cybersecurity goals. Organizations need to trace security requirements back to their security obligations and educate the people so they understand how their actions will make the organization more secure. Organizations need to show how poor security choices by any individual can have devastating business impacts for everyone.

Keep Score and Report

An organization's security argument can be made more compelling if it can back up the argument with facts taken from the organization's situation. Replace generic cybersecurity statements with specific examples drawn from the organization's own cyberdefense sensors. "Attackers are constantly probing" is much less compelling than "our organization was probed 5,000 times last month." Collect the metrics that tell the organization's security story, and then report that story to the organization's leadership and its people.

This technique is most often used to report bad news, but it can be used to report good news as well. Cyber personnel should also report on improvements to the organization's cyberdefense situation. Messages that cyberattacks are down, mistakes are less frequent, or vulnerability has been reduced, will likely be well-received by management.

Engage in an Active Defense

Regardless of how advanced an organization's technology or how small its security risk profile, cyberdefense cannot be a passive activity. An organization must be engaged in cyber operations, watching its tools for alerts and investigating when they indicate trouble. This recommendation does not mean that someone has to jump every time there is a port scan on the firewall. Rather, it means that someone needs to be monitoring security alerts, checking security logs, and following up when there are signs of real cyberattacker activities. When that trouble turns out to be a real attack, the organization needs to be prepared to support the cyber team in investigating, containing, and remediating that attack as quickly as possible.

Automate Cyberdefenses

In the future, cyberattacks will likely be smarter, faster, and more devastating. Machine speed attacks may take out entire organizations' IT environments in a matter of minutes. This type of attack may even target backup systems, cloud services, and network-connected devices. These advanced attacks may give little warning that they are about to occur, and even less time to respond once they start. Equally automated defenses will be able to recognize these attacks and counter them before they can succeed.

Build and Maintain Resilience

Even with the best defenses, things are going to go wrong. Missed patches, administrator mistakes, weak passwords, or the dreaded "zero day" attack may eventually cause organization protections to fail and things to go wrong. These situations are where resilience is critical. Resilience will allow the organization to absorb a failure, breach, or outage within an acceptable level of damage.

Resilience may involve limiting the scope of a single cloud account so that one compromised account won't take out all of IT. It may involve having isolated backup systems that can be brought online in the case of an outage. It may involve separating key financial accounts so that a financial attack can't take all of an organization's money. Or it may involve having cyber insurance and contingency plans so that an organization can get help when a crisis occurs. Most of all, resilience involves accepting that things may go wrong, making plans for the possibility, and making investments to support those plans.

Be Cautious, But Smart

Cybersecurity professionals and their partners who take on an organization's cybersecurity mission need to "be cautious, but smart." *What does that phrase mean?*

By being *cautious*, cybersecurity professionals need to champion the cause of security, even when others may want to ignore security in favor of other business goals. Cybersecurity professionals are the ones reminding people that mistakes will occur, accidents will happen, and things will go wrong. Cybersecurity professionals are the ones reminding people that "bad guys" and criminals will try to exploit the organization and steal its money, resources, or intellectual property. Cybersecurity professionals are the calm voice of cautious reason when

perhaps other voices are not. But there is more to just being cautious – cybersecurity professionals need to be smart, too.

By being *smart*, they understand that security does not happen in a vacuum and that there is more to security than just trying to lock down everything, all the time. While security may involve sometimes saying "no," it cannot be about *always* saying "no." Cybersecurity professionals need to understand the organization's business, larger business threats, and other business concerns besides cyber protection. Cybersecurity professionals need to use this perspective to define a security program appropriate for the organization, its business, and its needs. There is no sense in being cybersecure if the organization goes bankrupt in the process.

Cybersecurity professionals need to bring the same skepticism they have toward the business to the organization's cybersecurity vendors. There is no cybersecurity "silver bullet" that changes the game of cyberdefense by using a single, groundbreaking vendor's technology or service. While there are certainly many good cybersecurity solutions addressing cybersecurity needs for a wide range of situations, none of them is a comprehensive solution all by itself. The cybersecurity professional will have to bring together solutions for endpoints, mobile accounts, passwords, cryptography, networks, monitoring, and asset management, to name a few, and somehow get these solutions working together as an integrated cyber system. Then the organization will have to update that cyber system on a regular basis to counter new threats, protect new assets, or use the latest techniques. Throughout, the organization will have to perform these security activities within a business mandate that is constantly under pressure to increase capabilities, reduce costs, and "do more with less."

Cybersecurity professionals need to be *cautious*, but *smart* about an organization's cybersecurity in context of its business. They need to be cautious of the risks posed by cyberattacks against the organization, while being smart about how cyber capabilities can help the organization manage those risks.

Appendix A
Common Malware Threats

Malware is malicious software designed to compromise the *confidentiality*, *integrity*, or *availability* of data and IT systems. Malware generally shows evidence of one or more of the following behaviors:

- **Aggregation.** Malware illicitly collects user credentials from victim computers, systems, databases, or websites.
- **Concealment.** Malware tries to persist or stay hidden on the victim computer after attempts to remove it.
- **Exfiltration.** Malware collects data from the victim computer and sends it to another computer.
- **Proliferation.** Malware attempts to propagate from one victim computer to another.
- **Reconnaissance.** Malware monitors user behavior without the user's knowledge or consent.

Malware can exploit vulnerabilities in software code, system configurations, or security architectures. Some vulnerabilities are remediated through patches, while others may require significant system redesign or technology replacement. Complex organization IT environments can have thousands or even millions of vulnerabilities that cyberattackers can potentially exploit. There are literally millions of existing malware programs, and new ones are being developed every day. This appendix provides examples of some *common malware* examples and *common malware cyberattacks*, as depicted in Figure A.1.

Examples of Common Malware

From the viewpoint of a malware victim, malware is a significant cyber threat, ranging from annoying and surveilling to destructive and costly. From the viewpoint of a cyberattacker, malware is a powerful cyber tool that provides significant capabilities, ranging from subtle reconnaissance to blatant destruction. Some examples of common malware are briefly described as follows.

https://doi.org/10.1515/9781501506529-015

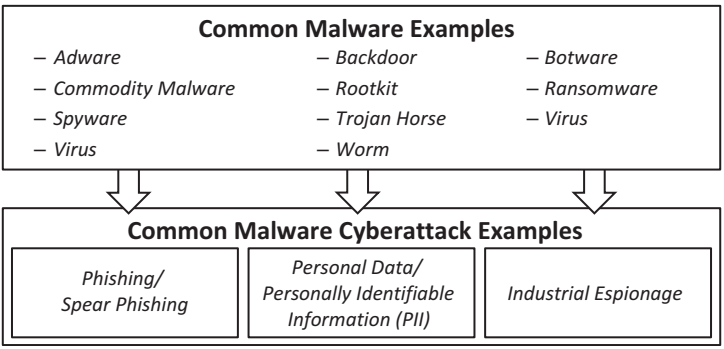


Figure A.1: Cyberattackers exploit vulnerabilities in software code, system configurations, and security architectures with a continually expanding set of malware tools and attack strategies.

Adware

A form of malware that installs itself on a computer and displays or downloads advertising material to the computer screen, or redirects a user's search request to advertising websites. Adware can collect location and marketing-type data about the user (such as websites they visited). Adware generates revenue for its developer by displaying advertisements to a computer. Adware may also be able to generate revenue for its developer when a user clicks on the displayed advertisements, or by making the victim's computer "click" on ads without the user's knowledge (click fraud). Adware is often used for legitimate uses, but it can become annoying due to unwanted pop-up advertisements. Sophisticated adware can disable a computer's anti-malware and virus protection, which can be downright dangerous.

Backdoor

A form of malware that is similar to Trojan horses or worms that provides a network connection for cyberattackers or other malware. This network connection then becomes a backdoor into the victim's network from the internet. The backdoor can then be used to gain remote access to the computer and its files, infect the computer with other malware tools, or send unsolicited junk e-mail (spam).

Botware

A form of malware that establishes a network of compromised computers (or an illegal "botnet") that are all under an attacker's central control. The illegal botnet can be used for malicious purposes such as conducting distributed denial of service (DDoS) attacks, emailing spam, or cryptojacking.

Commodity Malware

A form of malware that generally does not require modifications or enhancements to attack the most common vulnerabilities of software used across a wide range of devices, such as browsers or operating systems. These devices can provide access to potentially millions or billions of potential targets. Commodity malware is considered "opportunistic" in that it targets general victims versus specific individuals or groups of individuals. Consequently, commodity malware does not usually require social engineering techniques or extensive reconnaissance in order to achieve its objectives.

Rootkit

A hard-to-detect malware that modifies the operating system of the victim machine so that it has complete access to the system, its files, and its hardware. Rootkits usually load before the operating system, allowing them to bypass operating system protections like antivirus software. The malware can then give the attacker complete control either locally or over a network connection. Rootkits can be persistent across reboots and may even persist after reinstalling the operating system, by hiding within unused sectors of the system's hard drive or other storage.

Ransomware

A form of malware that encrypts data stored on the victim's computer and then demands a ransom to decrypt the data. If the user refuses to pay the ransom, the digital key that can decrypt the data is destroyed and the data is lost. Attackers frequently demand the ransom be paid using a cryptocurrency such as Bitcoin, which can be difficult or impossible to trace. More sophisticated ransomware versions will attempt to discover the victim's backups, databases, file

shares, and cloud storage. These more sophisticated versions will then attempt to encrypt and hold ransom all copies of the victim's data.

Spyware

A type of malware that does not usually affect a computer's performance, but collects information about the computer's activity and sends that information to a remote command-and-control system operated by the attacker. Spyware can collect data about web-surfing, program usage, e-mail activity, log-on credentials, and banking or other sensitive account information. Based on a user's internet activity, spyware may also send advertising to the user's computer.

Trojan Horse or Trojan

This dangerous form of malware appears to have a visible purpose when in fact, it has a hidden, malicious purpose. For example, free internet applications may offer useful utilities, but in reality, the applications are really Trojan horses designed to perform unwanted activities. Trojan horses may have hidden capabilities to display advertisements, change web-browser home pages, record user web-surfing habits, or capture log-on credentials, and then secretly report the results back to the attacker.

Virus

A replicating form of malware that attaches itself to other pieces of software in order to propagate and run. A virus can be embedded into an application or computer operating system, but it is unable to run on its own. It usually includes the ability to replicate itself when the infected application or operating system are run. A virus may also have a payload to perform some type of destructive or malicious behavior.

Worm

A destructive form of malware with the ability to run and replicate itself independently. This ability is in contrast to a virus, which requires a carrier to propagate and execute. Worms usually include the ability to replicate themselves

from system to system. Similar to viruses, worms may also have a payload to perform some type of destructive or malicious behavior, such as destroying data and files on the victim's computer.

Examples of Common Malware Cyberattacks

A malware cyberattack brings malware tools together with penetration and vulnerability exploitation to target a designated victim. Malware cyberattacks frequently have a business objective on the part of the attacker, whether it is to penetrate defenses, steal sensitive data, or achieve financial goals. Some examples of malware cyberattacks are briefly described as follows.

Phishing/Spear Phishing

These cyberattacks are some of the most effective ways of getting into an organization's network. Attackers send *phishing* e-mails to potential victims (e.g., employees) and *spear phishing* e-mails to a specific person (e.g., a senior executive). In either attack, the attacker's objective is to take control of the potential victim's computer through the malicious e-mail.

- **Impact.** Attackers take control of personal computers.
- **Methods and Consequences.** Attackers routinely use one or more of the following three phishing and spear phishing techniques in their e-mail messages:
  - A malicious attachment that takes control of the victim's computer when opened.
  - A link to a web page that exploits a vulnerability and takes control of the victim's computer.
  - A link to a web page that asks for the victim to type in the victim's logon credentials (i.e., username and password).

  Attackers can dramatically increase the likelihood of attack success by sending many related e-mails to the potential victims. Studies have found that after the third or fourth e-mail in the campaign, it becomes likely that the potential victim will click on one of the e-mails and possibly give control of their personal computer to the attackers.
- **Potential Defenses.** Training helps people recognize when they are being phished. For example, people should look for nonspecific greetings (e.g., "To Whom It May Concern"), inconsistent e-mail addresses where the sending e-mail address does not match the sending organization (e.g., a "FedEx" e-mail that does not originate from an "@fedex.com" e-mail address),

requests for personal information (e.g., telephone number, credit card number, or social security number), or offers that are too good to be true (e.g., a "dream vacation" for pennies on the dollar).

It is important to educate executives and systems administrators who often have access to privileged and regulated information that is far more sensitive than what the typical employee can access. These personnel should receive additional training on the threats specifically targeting them, their computers, and organization accounts. In addition, e-mail and web security controls can be installed on servers, web gateways, or delivered through cloud services to provide additional protection by blocking potentially malicious messages or websites.

Personal Data/Personally Identifiable Information (PII)

The European Union (EU) data privacy law, General Data Protection Regulation (GDPR),[1] defines *personal data* as follows:

> Article 4(1): '*personal data*' means *any information relating to an identified or identifiable natural person* [emphasis added] ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The US Government Accountability Office (GAO) Report 08–536, "PRIVACY – Alternatives Exist for Enhancing Protection of Personally Identifiable Information,"[2] defines *personally identifiable information (PII)* as follows:

> The terms *personal information* and *personally identifiable information* [emphasis added] are used interchangeably to refer to any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

---

1 General Data Protection Regulation (GDPR), Article 4 GDPR Definitions, https://gdpr.eu/article-4-definitions/.

2 General Accountability Office (GAO), *PRIVACY – Alternatives Exist for Enhancing Protection of Personally Identifiable Information*, GAO-Report 08–536, Washington, D.C.: May 19, 2008. https://www.gao.gov/products/gao-08-536.

Personal data and personally identifiable information (PII) theft are two of the most common professional cyberattacks because such data can be easily sold on the "dark web" criminal internet – particularly social security numbers, credit card numbers, and medical records. Such attacks tend to focus on centralized IT systems and databases. Attackers also target point-of-sale systems because they contain valuable identity information.

Experian reports that common pieces of personal information sell on the dark web for the following prices, as shown in Table A.1:[3]

Table A.1: Personal information is a valuable asset that can be used by cybercriminals for years.

Personal Information	Price on the Dark Web
Social Security Number	$1
Online Payment Login Information	$20 to $200
Credit or Debit Card	$5 to $110
Driver License	$20
Loyalty Accounts	$20
General Non-Financial Institution Logins	$1
Diplomas	$100 to $400
Passports (US)	$1,000 to $2,000
Subscription Services	$1 to $10
Medical Records	$1 to $1,000

- ***Impact.*** The impact of these personal information attacks can be severe for victim organizations because the data is frequently regulated. Data breaches can result in severe disclosure requirements, compensation to victims, and possibly penalties or fines as well. For example, the US Health Insurance Portability and Accountability Act (HIPAA) of 1996 defines many of the requirements for health care providers in terms of collecting, sharing, and protecting personal health information (PHI) when it is stored on paper or as electronic health records (EHRs). For HIPAA violations, the US Department of Health & Human Services (HSS), Office of Civil Rights (OCR) can levy fines that range from hundreds, thousands, or even millions of dollars. In addition, individuals (and their lawyers) may also sue the breached organization for additional damages.

3 Stack, Brian. "Here's How Much Your Personal Information Is Selling for on the Dark Web," Experian Consumer Services, Experian (December 6, 2017). Note: The value of information is related, in part, to its completeness and age.

- ***Methods and Consequences.*** Attackers use a number of techniques – such as phishing, ransomware, insider threats – to gain access to victim networks and get privileged access to victim data. Generally, these techniques take advantage of victims who do not have good visibility into their environments for detecting or protecting against attackers who have penetrated the outermost defensive layers. In addition, attackers may try to take advantage of the loss or theft of equipment used to house personal information or backups containing personal information.
- ***Potential Defenses.*** Protection against these attacks focuses on protecting the data involved, whether it is financial, medical, or identity data. Defenders should think through the life cycle of the data involved from capture to disposal, and consider the steps an attacker would need to take to intercept that data. Security revolves around making these steps both difficult for attackers to perform and easy for defenders to monitor. Defenders can also review their security practices regarding e-mail, hardening endpoints, access management, data loss and loss prevention, network management, and vulnerability management. Similarly, defenders should also review their manual processes, such as physically transporting backup data to offsite locations.

Industrial Espionage

This cyberattack is performed by professional and nation-state attackers to gain advantages in international business. Attackers penetrate victim networks to steal sensitive information (such as strategic business plans, operational databases, or confidential communications) and proprietary information (such as operational databases, patents, or trade secrets). Such information can be worth billions of dollars in the international marketplace or affect trade negotiations among competing countries. Industrial espionage may also include attackers shutting down online services or disabling manufacturing plants.[4] Reported victims of industrial espionage include organizations in every business sector including professional services, transportation, and manufacturing, to name a few.

- ***Impact.*** The impact of these attacks is difficult to measure, since it is often difficult to differentiate competition in a "healthy" marketplace based on "full and open" competition from competition in an "unhealthy" marketplace

4 While industrial espionage objectives are often associated with commercial cyberattackers, they may also be the objectives of nation-state and military attackers.

based on stolen competitor data, strategies, and processes. Organizations in a "healthy" marketplace may never find out if they lost key bids due to industrial espionage, or sincere competition. Upon losing core business due to industrial espionage, victim organizations may have to cut back on innovative research and development programs, lay off key talent, or re-align their business lines – further slowing their growth. It is difficult to place an economic impact value on industrial espionage, particularly when attackers successfully cover their tracks or go undetected.

- ***Methods and Consequences.*** Attackers generally target victim networks to achieve an initial entry, then exploit the entry to move laterally and gain privilege within the victim networks. Attackers may use social engineering techniques (e.g., phishing, spear phishing) to trick users into revealing credentials or privileged information as a first step toward achieving initial entry into an organization. Once the attackers have administrative control of the victim's environment, or at least the data they are targeting, attackers can steal the information they want and exfiltrate it out of the victim's IT environment.
- ***Potential Defenses.*** Preventive and detective security controls help protect an organization against industrial espionage attacks by defending along the cyberattack sequence. Preventive controls can effectively block undesirable behavior. Detective controls can complement preventive controls by providing the ability to detect malicious activities that the preventive controls failed to block. Response controls can then give defenders the ability to pursue active cyberattacks and take measures to repel the attackers from the environment. These controls should be layered so that such attacks cannot succeed without tripping multiple alarms and detectors. These alarms then give cyberdefenders an opportunity to respond to the attack before it can succeed.

Appendix B
Cyber Awareness and Cyber Training Topics

Personal cyber awareness involves thinking about how our daily actions affect our security posture at work, at home, and on travel. When we are cyber aware, we are continuously thinking about the security consequences of our actions. Organizational cyber awareness involves thinking about how the interwoven activities of personnel, customers, partners, service providers, vendors, and guests affect an organization's security posture.

Ever-present and evolving cyber threats require organizations to provide cyber training to their staff. As depicted in Figure B.1, there are many factors influencing an organization's cybersecurity program.

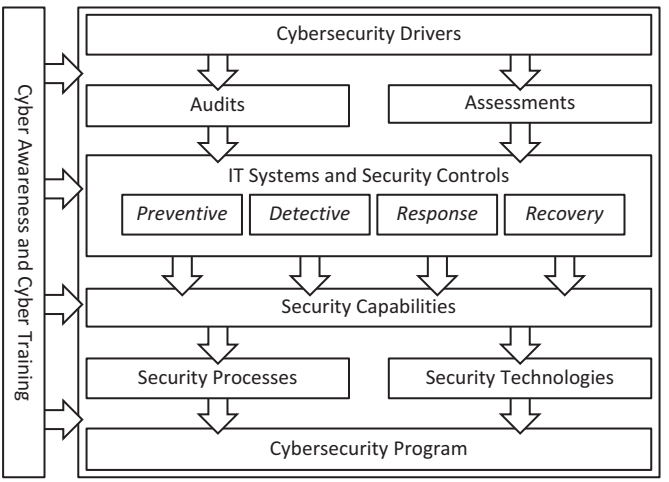


Figure B.1: Staying up to date on the latest cyberattacks, security trends, security controls, security capabilities, and corresponding responsibilities can be a daunting task.

Organizational training is more than annual or biannual occurrences, and more than a series of meetings or training exercises. To endure over time, cyber awareness, cyber training, and the corresponding best practices need to be an integral part of an organization's culture.

This appendix presents potential *cyber awareness* and *cyber training* topics for consideration when refining or developing an organization cyber training program. These lists of cyber training topics are grouped into the following categories: *cyber awareness environments*, *organization cyber awareness topics*, and *organization*

https://doi.org/10.1515/9781501506529-016

cyber training topics. These lists of cyber topics are not meant to be exhaustive, and are described in the following sections.

Cyber Awareness Environments

Figure B.2 depicts the following major *cyber awareness environments*: at work, at home, and on travel, and awareness topics within each of those environments.

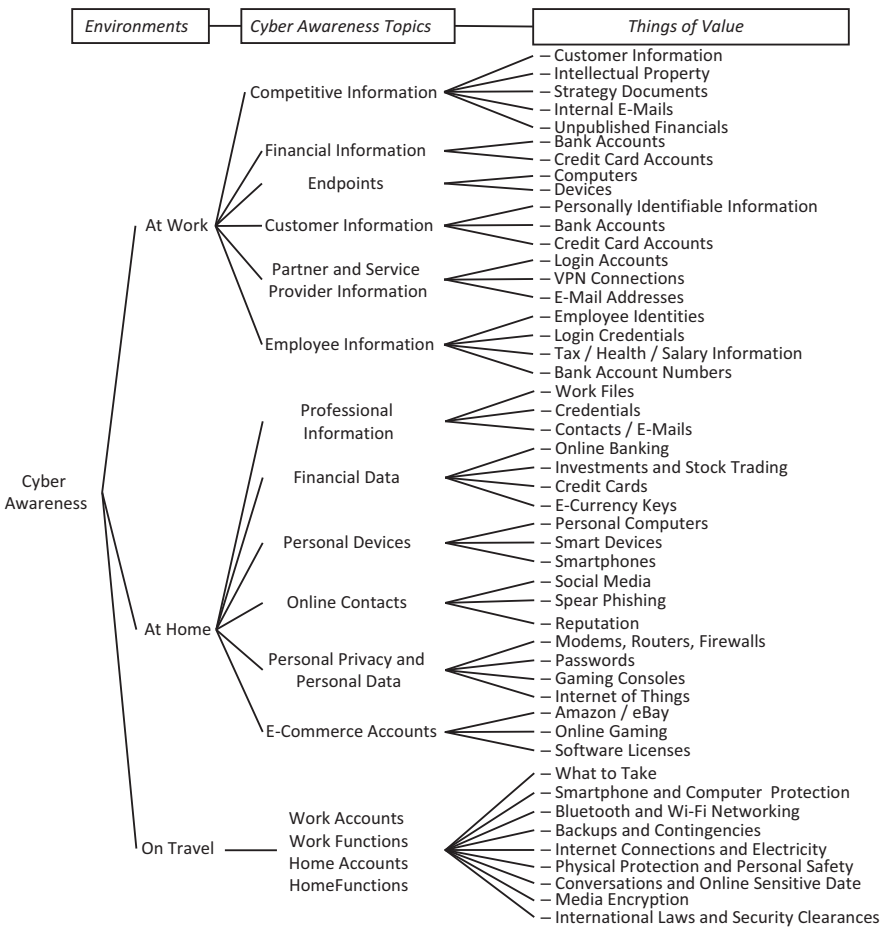


Figure B.2: Cyber awareness environments exist at work, at home, and on travel, where each environment has its own set of cyberattacks, which sometimes overlap other environments.

For each environment, Figure B.2 lists *cyber awareness topics* such as competitive information and financial information. For each topic, representative *things of value* such as customer information and intellectual property are listed.

Organization Cyber Awareness Topics

Figure B.3 depicts the following *organization cyber awareness topics*: personal versus organization cybersecurity; network perimeter and security; endpoint hardening and security; identity, authentication, and access management; web and e-mail protection; remote access to IT resources; cybersecurity operations;

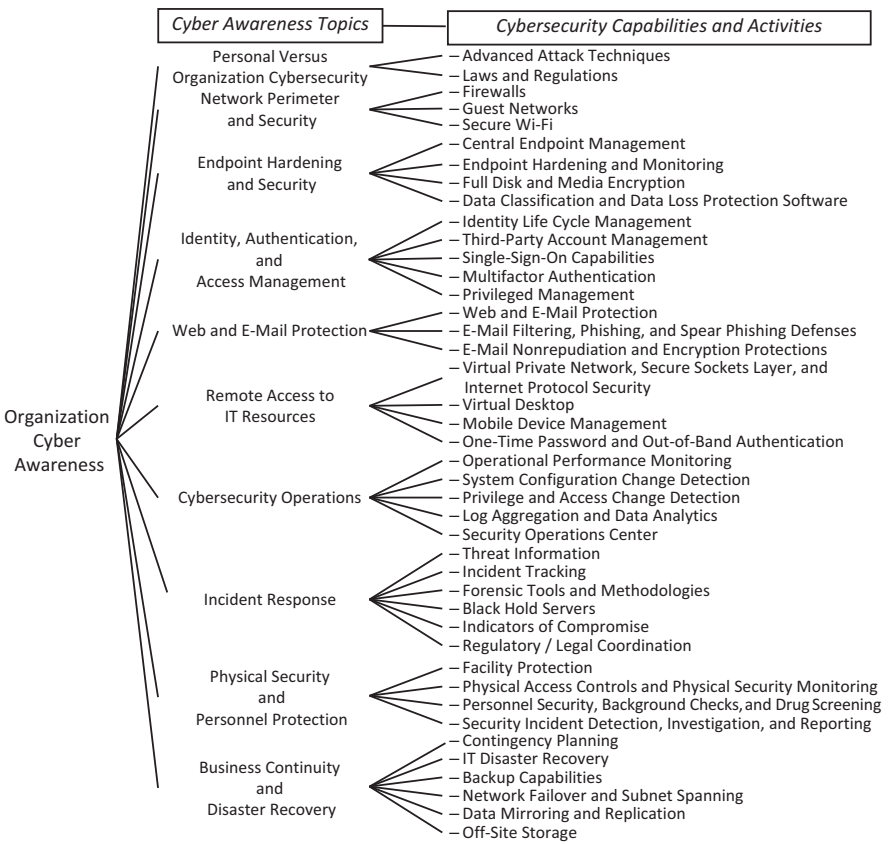


Figure B.3: Organization cyber awareness involves thinking about how the interwoven activities of personnel, customers, partners, service providers, vendors, and guests affect an organization's security posture.

incident response; physical security and personnel protection; and business continuity and disaster recovery. For each topic, representative examples of *cybersecurity capabilities and activities* such as advanced attack techniques, and laws and regulations are listed.

Organization Cyber Training Topics

Figure B.4 depicts the following *organization cyber training modules*: cyber training for everyone; cyber training for executives; cyber training for IT staff; cyber training for security staff; and cyber training for partners and specialists. For each module, representative examples of *cyber training topics* such as security mindset, and evolving malware and threats are listed.

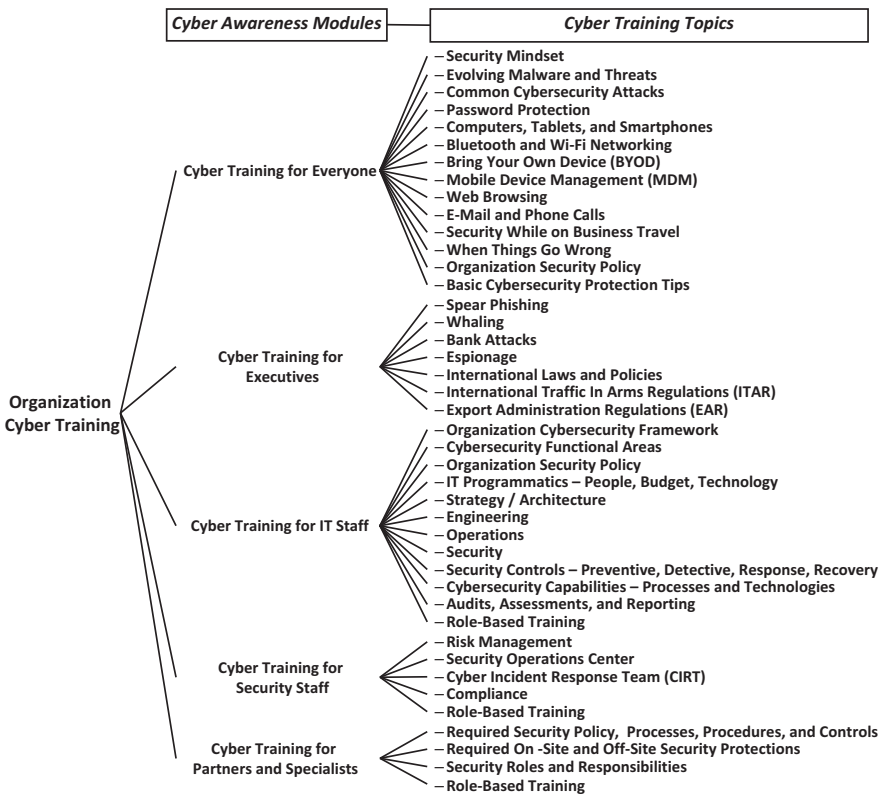


Figure B.4: Organization cyber training should provide the knowledge, shills, and abilities (KSAs) needed to build and maintain organization cybersecurity defenses.

Organization cyber training may be standalone training, or it may be integrated with other training on general security practices, business risk, or regulatory compliance. Such training should help employees be aware of the organization's cyber risks, how the organization can mitigate those risks, and the employees' responsibilities regarding those mitigations.

Senior executives should participate in communicating messages regarding the organization's training program to help set context and emphasize the rationale for an effective cybersecurity program. Executives can stress the importance of aligning cyber training to the organization's *cyber policy*,[1] which is a key component of its cybersecurity program.

1 See Appendix C, "Example Cyber Policy" for a detailed policy description.

Appendix C
Example Cyber Policy

This appendix provides an example cyber policy[1] for a notional organization requiring cybersecurity protection. As shown in Figure C.1, cyber policy is a key component of an organization's cybersecurity framework that helps to define its cybersecurity program.

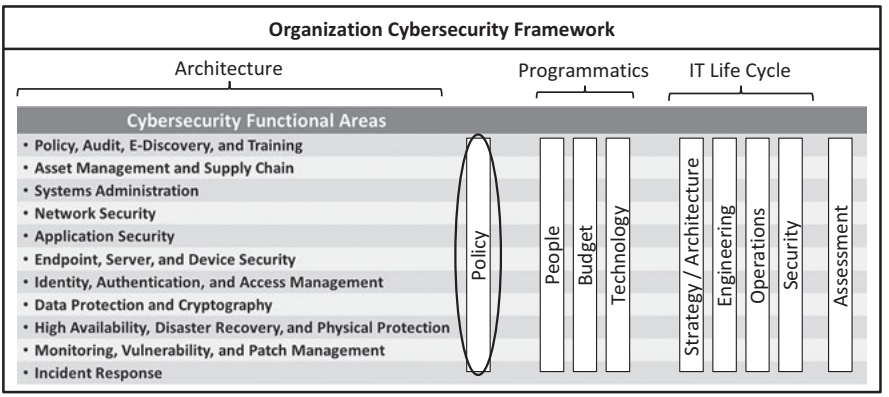


Figure C.1: An effective organization cybersecurity program begins with policy that is unambiguous, well-organized, well-maintained, and balances the security needs against business priorities.

Policy establishes the foundation upon which an organization's cybersecurity program is built, and represents a contract between the organization and its cybersecurity practice. Policy directs what is to be protected and to what degree, as well as what the consequences are for policy violations. People, budget, technology, and operations should all trace back to written policy. Linking these policy factors together provides a foundation for the entire cybersecurity program.

These policy factors are detailed through organizational standards, guidelines, processes, procedures, and baselines which can be defined as follows:

– *Standards* are documents specifying behavior, processes, configurations, or technologies to be used for organization cybersecurity.

1 This appendix is adapted, in part, from Donaldson, Scott E., Siegel, Stanley G., Williams. Chris K., and Aslam, Abdul. *Enterprise Cybersecurity Study Guide*, Apress, 2018.

https://doi.org/10.1515/9781501506529-017

- *Guidelines* are documents providing non-authoritative guidance on policy and standards for use by organizational elements.
- *Procedures* are documents describing step-by-step or detailed instructions for implementing, performing, or maintaining security controls.
- *Baselines* are specific configurations for technologies and systems designed to comply with the established policy, standards, guidelines, and procedures.

Figure C.2 depicts *representative* sections of a sample organizational cyber policy document. Policy requirements can be organized by functional areas to help ensure the policy is well-coordinated with an organization's people, budgets, technologies, IT life cycle, and cybersecurity assessments.

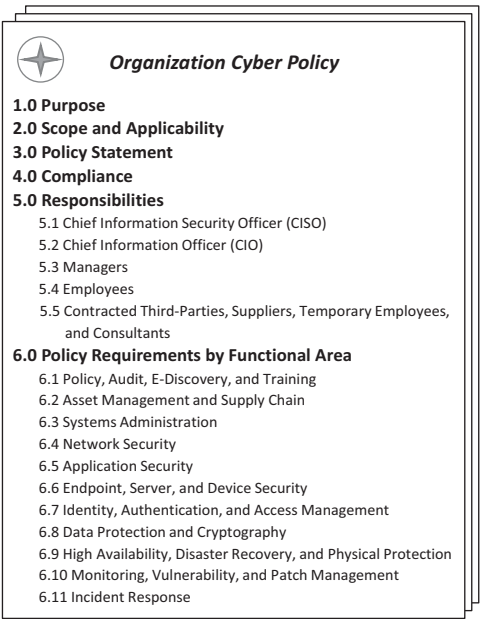


Figure C.2: This sample policy can be used as a starting point for creating a specific cyber policy documents tailored to an organization's mission and requirements.

The following material describes the sections of this sample organization cyber policy document.

1.0 Purpose

This policy delineates the cybersecurity requirements, roles, responsibilities, training, and functional area security guidance necessary to protect organizational data and information systems from unauthorized access, inappropriate disclosure, or compromise. This policy was developed, reviewed, and approved in accordance with established organization processes to ensure governing laws, regulations, industry-appropriate standards, organization liability obligations, and corporate responsibilities are correctly incorporated.

The cyber policy should be defined in context of organization ownership that includes publicly traded companies, government-run organizations, or privately held organizations.

This policy must be used to assess the risk of conducting organization business, and to identify appropriate business and cybersecurity controls for mitigating that risk to acceptable levels.

2.0 Scope and Applicability

This policy applies to all employees, temporary employees, contracted third-parties, suppliers, consultants, and organization subsidiaries. Exceptions to this policy must be approved by the chief executive officer (CEO) in consultation with the chief information security officer (CISO), chief information officer (CIO), and other management, as dictated by organization policies.[2] This policy must be reviewed and revised on an annual basis (or more frequently) in accordance with organization policies and procedures.

3.0 Policy Statement

This policy:

- Complies with organization data protection requirements as stated by governing laws, regulations, and contractual obligations. When such requirements

---

2 Cybersecurity policy exceptions do not *have* to go to the CEO, but they should go to appropriate executive levels for adjudication and approval. It is very important that there be a formal process for requesting, approving, tracking, and re-certifying exceptions to cybersecurity policy, as a part of the organization's overall cybersecurity program.

exceed this policy's stipulations, requirements of the laws, regulations, or contractual obligations shall take precedence.
- Provides the authority to design, implement, and maintain security controls in accordance with the organization's standards for protection of data at rest, data in motion, and data processed by information systems.
- Requires organization data to be stored and used on organization-provided information systems or contracted systems that are approved for use and that comply with this policy.
- Mandates that employees comply with this policy and undergo required security training on the security topics delineated in this policy.
- Informs employees that the organization may monitor their usage of the organization's information systems and hosted data.
- Implements a security incident reporting mechanism to securely identify incidents such as policy violations, potential data breaches, fraud, intrusions to information systems, and theft of hardware, software, or data.

4.0 Compliance

Failure to comply with this policy may result in disciplinary action, such as the removal or limitation of access to organization systems, termination of employment or contractual agreements, letters of reprimand, or unfavorable employee performance reviews. Such failures could have legal or regulatory ramifications with regard to federal, state, local, or international law.

Organization security and internal/external audit teams may conduct periodic assessments to confirm compliance with this policy. Organization elements and project teams should conduct periodic self-assessments to identify potential compliance gaps requiring remediation.

5.0 Responsibilities

This section identifies responsibilities for key roles within the organization's cybersecurity program and cybersecurity policy compliance efforts.

5.1 Chief Information Security Officer (CISO)

- Acts as primary custodian of the cyber risk assessment process.
- Reports identified risk to the organization risk committee and other key stakeholders.
- Keeps the organization security policy and procedures current for both digital and physical assets.
- Publishes up-to-date security standards.
- Acts as the incident lead during an active incident and submits an after-action incident root cause report to management.
- Enforces compliance with organization security policies by conducting periodic security checks and audits.
- Ensures that identified system vulnerabilities are mitigated in a timely manner.
- Oversees internal and external reporting requirements, such as, Sarbanes-Oxley (SOX), Security and Exchange Commission (SEC), and Health Insurance Portability and Accountability Act (HIPAA).
- Interfaces with the legal department to support e-discovery.
- Implements security awareness and training campaigns.
- Supports the due diligence process for vetting security quality of suppliers, products, and subsidiaries during mergers and acquisitions.

5.2 Chief Information Officer (CIO)

- Provides the governance for organization IT systems and information with respect to security compliance with this policy.
- Publishes a common operating environment (COE) that defines infrastructure standards incorporating security policies.
- Reviews and approves any low-risk COE deviations or exceptions.
- Provides guidelines for on-and-off-network information systems with respect to maintaining an information security plan.

5.3 Managers

- Comply with the organization's security policies.
- Ensure that employee security training is completed.
- Follow established incident reporting and escalation procedures.
- Periodically update standard operating procedures (SOPs) to ensure compliance with organization policy and procedures.

5.4 Employees

- Comply with organization security policy and procedures.
- Complete required security training.
- Follow established incident reporting and escalation procedures.
- Protect their organization-provided equipment and access credentials in accordance with organization policy.

5.5 Contracted Third-Parties, Suppliers, Temporary Employees, Consultants

- Must demonstrate that they can meet and perform per organization policy and procedures.
- Provide the organization with required third-party audit reports as part of due care.
- Inform the organization of security-related concerns or cybersecurity incidents related to their delivery of services to the organization.

6.0 Policy Requirements by Functional Area

This appendix describes specific technical requirements of the organization's cybersecurity policy. These requirements are organized by functional area, for reference and implementation.

6.1 Policy, Audit, E-Discovery, and Training

This functional area deals with the governance of cybersecurity policy, audit, e-discovery, and training. The functional area maintains cybersecurity policies, conducts periodic audits of security controls and protections, provides support for legal e-discovery activities, and maintains up-to-date training of cybersecurity personnel, employees, and contractors in proper cybersecurity practices and techniques.

Required activities for this functional area include the following:

- Obtain approval of organization cybersecurity policy by business leadership with inputs from key stakeholders to include legal, contracts, IT, and cybersecurity departments.
- Establish a formal security forum to enable key stakeholders to discuss security matters on a regular basis and document policy changes or enhancement recommendations.

- Track cybersecurity risks and their potential business consequences.
- Report on cybersecurity risks and their mitigation on a periodic basis (e.g., quarterly).
- Provide cybersecurity governance, risk management, and compliance reporting to ensure legal, regulatory, and contractual requirements are met.
- Comply with legal, regulatory, and contractual requirements stipulated by Sarbanes-Oxley (SOX), Payment Card Industry (PCI), Health Information Portability and Accountability Act (HIPAA).
- Comply with documented requests for e-discovery originating from the legal department and retain documentation for a set period (e.g., seven years).
- Document, track, and re-certify exceptions to cybersecurity policies on a periodic basis (e.g., annually).
- Remove policy exceptions that are not re-certified and enforce the policy.
- Comply with customer and internal requirements for information system Certification and Accreditation (C&A), as specified in customer contracts and internal memorandum of understanding (MOUs).
- Audit *all* cybersecurity preventive, detective, audit, and forensic controls on a periodic basis (e.g., annually) to ensure their proper design and operation.

Within this functional area, mandatory review, validation, testing, and training activities include the following:

- Review policy, audit, e-discovery and training programs on a periodic basis (e.g., annually), including re-validation of all policy exceptions.
- Verify and test policy, audit, e-discovery and training controls (preventive, detective, audit, and forensic) for proper operation on a periodic basis (e.g., at least annually).
- Ensure that all employees receive annual training on cybersecurity concerns and obligations.
- Provide additional training suitable for the roles of employees in positions of trust, including executives and systems administrators.

6.2 Asset Management and Supply Chain

This functional area provides for the accounting of organization assets, procurement information associated with them, their life cycles, changes, and ensuring orderly and secure disposal without compromise of organization data or security. It is critical that asset information be kept current to support IT operation and handling of cybersecurity incidents. A supply chain management program must account for both products and services. The program must include

security assessment, periodic re-assessment, and inclusion of supplier information in the asset management database.

Required activities for this functional area include the following:

- Assign all software and hardware assets to an organization system with a primary and alternate employee point of contact. Update points of contact when personnel change or are re-assigned.
- Use a centralized asset management system to track all organization hardware and software assets from their acquisition through to their disposal.
- Use a centralized configuration and change management system to perform the following activities:
  - Track configurations of organization hardware and software systems.
  - Track the approval of changes to those configurations.
  - Detect unauthorized changes to those configurations when such changes occur.
- Track organization software licenses and software utilization to perform the following activities:
  - Match software licenses with utilization.
  - Ensure software license compliance.
  - Identify and remediate unauthorized software in the organization.
- Review and approve vendors and suppliers as part of system acquisition, and categorize their associated risks as "identified," "accepted," or "mitigated."
- Properly dispose of hardware and software assets retired from service by performing the following activities:
  - Release the software licenses and terminate the software and hardware support contracts.
  - Sanitize or destroy hardware persistent storage (e.g., flash and hard drive storage) to protect organization data.
  - Remove assets from the asset and configuration databases upon successful completion of the above activities.
- Sanitize persistent storage media, including flash drives, portable media, hard drives, and device-embedded storage (such as copiers and voicemail appliances with data storage features) of organization data using the following methods:
  - Physical destruction.
  - Data cleaning.
  - Data scrubbing.
  - Data encryption methods such that data may not be recovered after disposal.

Within this functional area, mandatory review, validation, testing, and training activities include the following:

- Validate data disposal methods periodically (e.g., annually) to ensure their effectiveness.
- Validate data encryption methods to ensure that the encryption strength is adequate to protect data for a set period (e.g., ten years) following disposal.
- Report loss or unintended disposal of equipment or disclosure of data as a cybersecurity incident.
- Inventory hardware and software assets periodically (e.g., annually), with all associated points of contact validated and updated as necessary.
- Review and update hardware, software, and service provider risk evaluations periodically (e.g., annually) or when changes occur that materially affect the security posture, such as cybersecurity incidents or breaches, mergers, divestitures, bankruptcies, and foreign acquisitions.
- Review asset management and supply chain configurations periodically (e.g., annually), including re-validation of all policy exceptions.
- Verify and test asset management and supply chain preventive, detective, audit, and forensic controls for proper operation periodically (e.g., at least annually).

6.3 Systems Administration

This functional area provides for secure administration of organization infrastructure and security systems, and protects systems administration channels from compromise. Systems administration is a critical function that provides management of sensitive organization information. If malicious actors compromise systems administration, they may gain almost unlimited access to the organization's data and information systems.

Required activities for this functional area include the following:

- Require authentication and record all log-ons to systems administration systems at the application, data, and operating system levels.
- Only use systems administration protocols that are secured by encryption and authentication protections.
- Only use systems administration protocols that are insecure or vulnerable to attack if they can be relegated to *isolated* networks with additional protections delivered at the network layer.
- Require multifactor authentication before administrative access is granted to systems administration accounts.

- Monitor systems administrator activities for signs of inappropriate activity and investigate such signs within seven days of occurrence.

Within this functional area, mandatory review, validation, testing, and training activities include the following:

- Record and audit systems administrator log-ons weekly.
- Verify systems administrator access control lists quarterly to ensure the enforcement of least privilege and separation of duties, where appropriate.
- Record and audit all changes to systems administrator access control list on a weekly basis.
- Review systems administrator security configurations and re-validate policy exceptions on an annual basis.
- Verify and test systems administrator preventive, detective, audit, and forensic controls for proper operation at least annually.

6.4 Network Security

This functional area provides for security of organization networks, their services, and access to them from the internet and internally connected devices. Network security examines data traversing the network to detect intrusions against the network and connected computers. Network security uses preventive controls, detective controls, and monitoring controls to defend the network. It is critical for the organization to protect the data and information systems connected to its networks from both external and internal malicious actors.

Required activities for this functional area include the following:

- Centrally manage network and network security infrastructure, including routers, switches, firewalls, and other networking equipment.
- Log all network and network security infrastructure log-ons for audit.
- Isolate network infrastructure administration activities from general business network traffic.
- Require credentials and multifactor authentication for all network administrative log-ons.
- Use access control for networks that might be publicly accessible or not physically protected, such as wireless networks and network connections in public spaces and conference rooms, to ensure only authorized users are permitted access.
- Detect and block network traffic known to be malicious, either through its protocols, its payloads, or its sources or destination, within one business day of detection.

- Require multifactor authentication for access to organization networks from the internet.
- Do not permit access to privileged internal networks directly from the internet.
- Harden the network infrastructure that provides for basic services – including name server, host configuration, and time synchronization – to protect them from attack or compromise.
- Require approval for network configuration changes and log such changes for audit and investigation as required.

Within this functional area, mandatory review, validation, testing, and training activities include the following:

- Review network security configurations and re-validate all network policy configuration exceptions on an annual basis.
- Verify and test network security preventive, detective, audit, and forensic controls for proper operation at least annually.
- Record and retain questionable network traffic (which may be indicative of attacks) for 90 days to permit analysis and investigation after the fact.

6.5 Application Security

This functional area provides for the security of organization applications using security technologies that are appropriate for and tailored to the protection of application vulnerabilities. The applications most needing additional security communicate over the network and are accessible from the internet. The organization must protect these applications from attack, and detect attacks and vulnerabilities in these applications when they occur.

Required activities for this functional area include the following:

- Protect internet-facing application servers from unauthorized configuration changes by logging and auditing configuration changes to catch the introduction of unauthorized "backdoors" into these systems.
- Configure critical organization applications – such as e-mail, voicemail, collaboration, and internal and external web services – to prevent and detect attacks and exploits of vulnerabilities.
- Maintain adequate forensic logs for attacks and exploits that are not prevented or detected to permit audit and investigation after the fact.
- Require authentication and secure protocols for communication between application components over open networks. Where such protection is not feasible, utilize alternative protection methods to protect these connections from attack.

- Employ protection and detection for applications sensitive to *confidentiality* concerns to protect against data leakage.
- Employ data integrity protections – such as digital signatures and data modification audit trails – for applications sensitive to *integrity* concerns to protect and detect against data changes.
- Employ high availability and rapid disaster recovery for applications sensitive to *availability* concerns to protect them from denial of service attacks originating internally and from the internet.

Within this functional area, mandatory review, validation, testing, and training activities include the following:

- At least quarterly, analyze the source code of custom applications using static code analysis. Address or remediate all medium and higher vulnerabilities.
- On a monthly basis, scan applications generally available on the internet or organization internal networks for vulnerabilities using a credentialed vulnerability scanner. Address or remediate all medium and higher vulnerabilities within 90 days of discovery.
- Temporarily or permanently disconnect applications found to be in violation of policy from the internet and/or the organization network until the violations can be remediated.
- Review application security configurations, including re-validation of all policy exceptions, on an annual basis.
- Verify and test application security preventive, detective, audit, and forensic controls for proper operation at least annually.

6.6 Endpoint, Server, and Device Security

This functional area provides for the protection of endpoint computing devices, such as personal computers, servers, and mobile devices that access organization data. This functional area also involves detecting when endpoints' defenses are breached. Endpoints must be hardened and secured using standard vendor recommended security guides and builds.

Required activities for this functional area include the following:

- Use unique local administrator account passwords or keys for each endpoint. Consider organization endpoint management capabilities to be critical security infrastructure and give them appropriate protections.
- Configure organization endpoints and servers from master images that are configuration-controlled and protected from tampering, changes, or the introduction of unauthorized or malicious code.

- Configure network-connected endpoint systems to forward security logs – including administrator log-on and security component configurations – to a central infrastructure for aggregation and correlation.
- Encrypt built-in and removable media of all portable and removable endpoints – personal computers, laptops, and mobile devices – so that such media cannot be accessed without proper authentication to the device.
- Configure endpoint systems for investigation of cybersecurity incidents by installing forensic tools and configuring security logs to meet the needs of incident investigators.
- Configure endpoint systems according to vendor-approved security guidelines for secure operating system installation and operation.
- Include endpoint protection for endpoint systems to block and detect malicious software and network connectivity, as appropriate to the security posture of the system. Endpoints involved in high-security functions may be configured for more restrictive security than general-use endpoints.
- Configure endpoints and servers involved in operating or managing organization cybersecurity functions for maximum restrictiveness, including security tools such as application whitelisting and session recording.
- Include the ability to remotely delete organization data from compromised personal computers and mobile devices when they are used for organization work. If this remote delete capability is not available, the system must include safeguards to ensure organization data is not stored on the device in a persistent state, or is encrypted to prevent unauthorized access.
- Include the ability to detect and alert on changes to security configuration files within one hour of changes occurring.
- On a monthly basis, scan servers directly connected to the internet for operating system vulnerabilities using a credentialed vulnerability scanner. Address and remediate all medium or higher operating system vulnerabilities within 30 days of discovery.
- Temporarily or permanently disconnect endpoints found to be in violation of policy from the organization network until the violation is remediated.

Within this functional area, mandatory review, validation, testing, and training activities include the following:

- Review endpoint server and device security configurations on an annual basis, including re-validation of all policy exceptions.
- Verify and test endpoint, server, and device security preventive, detective, audit, and forensic controls for proper operation at least annually.

6.7 Identity, Authentication, and Access Management

This functional area provides support to all other security functional areas by providing answers to the following questions:

- *Who is accessing organization IT systems?*
- *How are they identified?*
- *What can they access once they are authorized?*

Required activities for this functional area include the following:

- Use centralized identity provisioning and de-provisioning, and centralized access management, where possible, for all production organization systems. Organization cloud-based systems and software-as-a-service solutions are subject to this policy, as well as on-premise systems.
- Protect identity systems at the same or greater level as the sensitivity of the communities and applications that they serve.
- Use identity systems to provide protective, detective, audit, and forensic controls governing all administrative changes to identity systems and all identity life cycle actions, such as account provisioning, de-provisioning, and changes.
- Use identity systems to alert on suspected attacker activities, including using privileged accounts on non-privileged systems, patterns of excessive log-ons, or log-on attempts that may be malicious.
- De-provision electronic identities no longer needed within 180 days.
- Sponsor electronic identities and permissions held by non-employees by at least one employee and re-certify every 90 days, or deprovision the identities and permissions.
- Use identity systems to support the protocols required for authentication and access control on organization systems, including on-premise and cloud-based systems.
- Support multifactor authentication for access to organization systems and applications from untrusted networks such as the internet, and for all uses of privileged systems administrator accounts on all networks.
- Include a delay for failed log-ons so that no more than five failed log-ons can be performed within one hour. Generate an alert requiring investigation before the account can be used for an account with more than ten failed log-on attempts.

Within this functional area, mandatory review, validation, testing, and training activities include the following:

- Review identity, authentication, and access management security configurations – including re-validation of all policy exceptions – on an annual basis.
- Verify and test identity, authentication, and access management preventive, detective, audit, and forensic controls for proper operation at least annually.

Passwords, when used for authentication, are subject to the following mandatory requirements:

- Change passwords actively used by users every 90 days, and the past ten passwords must be unique.
- Change passwords internal to systems and not used interactively by users annually, and the past ten passwords must be unique.
- Use only passwords at least twelve characters long, and encourage longer pass phrases. Make sure pass phrases containing spaces are supported by all applications requiring authentication.
- Use only passwords containing uppercase, lowercase, and a number or a special character. Verify password policy works on all applications.
- Do not use passwords containing internal repetitions to allow them to meet length requirements (e.g., PasswordPassword1).
- Do not display passwords in clear text during the log-in process.
- Do not write down user passwords on paper or store them in unencrypted computer files.
- Physically protect system account passwords in a locked safe or password management system. Encrypt and access control passwords electronically stored on network-accessible systems. Require multifactor authentication for user access if a single electronic system or database contains more than 100 system passwords.
- When passwords must be generated and transmitted, encrypt the transmission or verbally transmit such passwords over the telephone. Only one-time passwords may be transmitted over insecure channels.
- Change compromised passwords immediately upon discovery.

With regard to password management, mandatory review, validation, and testing activities include the following:

- Review password security configurations, including re-validation of all policy exceptions, on an annual basis.
- Verify and test password preventive, detective, audit, and forensic controls for proper operation at least annually.
- Periodically review password length and complexity requirements, to ensure they are adequate to resist modern brute force attack methods.

6.8 Data Protection and Cryptography

This functional area provides for the protection of data stored in the organization and the use of cryptographic technologies to perform that protection. It also includes the use of cryptography to support other operations such as authentication, non-repudiation, or data integrity. Cryptography may also be critical to the effectiveness of strong authentication technologies such as digital certificates, smart cards, and one-time password tokens.

Required activities for this functional area include the following:

- Protect sensitive data transmissions using Secure Sockets Layer (SSL), Transport Layer Security (TLS), Internet Protocol Security (IPSec), or equivalent secure protocols on both internal protected networks and insecure networks such as the internet.
- Ensure that encryption modules, algorithms, and protocols meet US National Institute of Standards and Technology (NIST) requirements as documented in approved Federal Information Processing Standards (FIPS) documents. International organizations may substitute appropriate international or local standards for cryptographic security.
- Use cryptographic algorithms rated to resist brute-force attack for a period of ten years at the time of use by an attacker with $10,000 worth of computing capacity, or other appropriate measures.
- Use cryptographic algorithms rated to resist an attacker with $100,000 or $1,000,000 worth of computer power for more sensitive operations. Note that as technology improves and costs drop, the amount of computing power this amount purchases will increase over time, mandating periodic upgrades.
- Define password policy using cryptographic principles based upon the amount of entropy required and the ability of brute-force attacks to be detected or delayed. Use these factors to design password complexity and rotation policy so attackers have less than a 1% chance of successfully guessing a password within its usable lifetime. Note that passwords with longer lifetimes will require commensurately greater complexity to resist brute-force attacks.
- Remediate published cryptographic vulnerabilities within 30 days of publication, or put compensating preventive or detective controls in place so that attempted exploits are blocked or at least detected.
- Centrally escrow and retain encryption keys for a period of seven years after the date of last use to support investigations by organization security, legal, or law enforcement personnel.
- Physically protect all non-public organization data at rest in a locked facility or container, or encrypt such data using cryptographic keys that are separate from the data, such as a strong password or encryption token.

- Adequately log data encryption separate from the media itself to permit investigators to validate that lost media was in fact encrypted at the time of loss.
- Use strong and multifactor authentication cryptographic methods to make authentication resistant to keylogging, replay, session hijacking, and brute-force attacks. Use cryptographic methods such as digital certificates, one-time passwords, and secure cryptographic modules for storing persistent private asymmetric and shared symmetric keys.
- Protect persistent keys used for strong authentication or persistent encryption using Hardware Security Modules (HSMs), Trusted Platform Modules (TPMs), secure elements, or smart cards that resist physical and logical attack to extract the keys.
- Do not require hardware protection for session encryption (such as that used by SSL, TLS, or IPSec), except where compromise of specific communication sessions would pose a significant organizational risk.

Within this functional area, mandatory review, validation, testing, and training activities include the following:

- Review data protection and cryptography modules, algorithms, protocols, and security configurations – including re-validation of all policy exceptions – on an annual basis.
- Verify and test data protection and cryptography preventive, detective, audit, and forensic controls for proper operation at least annually.

6.9 High Availability, Disaster Recovery, and Physical Protection

This functional area provides for the protection of organization IT services being available for use by legitimate users. This functional area helps to make IT systems highly available and recoverable from disasters. This functional area also provides physical protections for facilities, people, systems, and data. Under the policy of this functional area, services, applications, and servers shall be configured with adequate redundancy and protection to meet business needs and ensure cost-effective service delivery in the event of accidental or deliberate incidents targeting their availability.

Required activities for this functional area include the following:

- Ensure that revenue-generating systems must have at least 99.99% availability and that other business IT systems must have at least 99.9% availability. Determine if supporting infrastructure may be subject to higher availability requirements as needed by the business.

- Recovery Point Objectives (RPOs) in the event of natural or humanmade disaster:
  - Ensure the RPOs for revenue-generating and business financial systems recover all committed transactions with customers or vendors that have financial consequences.
  - Ensure other business IT systems' RPOs recover data up to the day before the incident (daily backups).
- Recovery Time Objectives (RTOs) in the event of natural or humanmade disaster:
  - Ensure the RTOs for revenue-generating business functions recover and achieve initial operating capability within seven days.
  - Ensure the RTOs for business financial systems recover to initial operating capability within 45 days.
  - Ensure the RTOs for other business systems recover to initial operating capability within 90 days.
  - Ensure RTO planning considers the time required for rebuilding affected servers, in addition to the time required for restoring data.
- Include adequate backups for major system upgrades and configuration changes to "roll back" the changes within the availability, recovery point, and recovery time requirements.
- Sufficiently protect backup data so that natural or humanmade disasters do not result in the destruction of both the primary copy and the backup.
- Encrypt backup data taken offsite, and sufficiently protect the backup data keys from loss or compromise so the backup data can be recovered even in the event of a catastrophic loss.
- Report the theft or loss of any organization-furnished equipment to the incident response team as soon as possible.
- Physically protect organization-sensitive data printed on paper or other materials in a locked room or cabinet.
- Include physical protection, monitoring, and detective controls for organization facilities and data centers to protect personnel and equipment from harm and accidents. Protect sensitive data and systems handling it in an unencrypted fashion using double-barrier protection and need-to-know access controls.
- Ensure that any third-party access to data centers is approved by data center operations supervisors, and escort guests during their visit.
- When automated physical access controls are used at organization facilities, maintain the access logs for one year to support investigations by audit, security, legal, and law enforcement personnel. Monitor logs 24/7 to detect intrusions and intrusion attempts.

Within this functional area, mandatory review, validation, testing, and training activities include the following:

- Test backup media, replication processes, and snapshot procedures annually to verify their proper operation.
- Test disaster recovery and service continuity plans using a drill, rehearsal, or tabletop practical exercise every two years to ensure their effectiveness.
- Conduct physical security risk assessments for all data centers, server rooms, and server closets on an annual basis.
- Review high availability, disaster recovery, and physical protection security configurations – including re-validation of all policy exceptions – on an annual basis.
- Verify and test high availability, disaster recovery, and physical protection preventive, detective, audit, and forensic controls for proper operation at least annually.

6.10 Monitoring, Vulnerability, and Patch Management

This functional area provides for the regular monitoring of security infrastructure, scanning and analysis of vulnerabilities in that infrastructure, and management of patches and workarounds to address those vulnerabilities. This functional area supports organization operational processes, in part, by identifying or detecting security concerns and alerts so they can be acted upon.

Required activities for this functional area include the following:

- Monitor organization systems and cloud services delivering business-critical functions for performance and availability so that failures can be detected within at least 30 minutes of their occurrence.
- Forward organization systems and cloud services logs to a central system for correlation and analysis. Provide for in-place analysis and alerting that ties in with organization incident detection and investigation services.
- Synchronize all log entries to Coordinated Universal Time (UTC) or a clearly delineated global time zone so that the times when events occur are clearly presented to investigators.
- Use security audit logging activities to clearly tie user activity in the information systems to named user or service accounts.
- Protect security audit logs from tampering and make them available to support investigations for a period of one year after the event is logged. Retain event logs related to public company financial activities for seven years after the events are logged.

- Monitor networks to detect rogue or malicious devices connecting to them. Configure wireless networks to detect attacks and rogue wireless access points.
- As needed, use detective technologies such as honeypots, honeynets, and honeytokens to detect attacker exploits of vulnerabilities and identify attacker tools, techniques, and procedures (TTPs).
- Feed system security monitoring into a central system for correlation that is monitored 24/7 to detect security incidents. Monitor security logs for activities known or suspected to be malicious. Generate security alerts within 30 minutes of such activity occurring.
- Scan new applications and servers for vulnerabilities and address all medium or higher vulnerabilities prior to becoming operational.
- Scan organization applications generally available on the internet or organization internal networks for vulnerabilities using a credentialed vulnerability scanner monthly. Address and remediate all medium or higher application vulnerabilities within 90 days of discovery. For sensitive systems with a significant business impact, the remediation window may be shorter – as short as one day.
- At least monthly, scan servers directly connected to the internet for operating system vulnerabilities using a credentialed vulnerability scanner. Address or remediate all medium or higher operating system vulnerabilities within 30 days of discovery. For sensitive systems with a significant business impact, the remediation window may be shorter – as short as six hours.
- Ensure that applications and systems in violation of vulnerability remediation policy shall be disconnected from the internet and organization networks until remediation can be performed and validated.
- Evaluate and install vendor-provided patches as recommended by vendors. Handle vulnerabilities relating to missing patches as per vulnerability policy. Employ mitigating preventive and detective controls when security patches cannot be installed for operational reasons.
- Assign patching as a responsibility to the system owner. When appropriate, use automated systems to simplify patch deployment, but limitations in these systems must be compensated for using manual techniques to ensure that security vulnerabilities are addressed in a timely manner.
- Configure detective controls to detect attacker exploits of known vulnerabilities when such configuration is technically possible.

Within this functional area, mandatory review, validation, testing, and training activities include the following:

- Perform penetration testing on internet-facing and user networks to identify vulnerabilities related to real-world attacker techniques on at least a

quarterly basis. Where critical vulnerabilities are identified, perform follow-up testing to verify systems have not been compromised.
- Review monitoring, vulnerability, and patch management security configurations – including re-validation of all policy exceptions – on an annual basis.
- Verify and test monitoring, vulnerability, and patch management preventive, detective, audit, and forensic controls for proper operation at least annually.

6.11 Incident Response

This functional area provides for the investigation, response, and recovery of incidents that are identified through monitoring of the organization. A security incident is any malicious event (perceived or real) performed against the organization's information systems or data contained within those information systems. An incident can originate within the organization (insider threat), in external entities, or in the surrounding environment.

When a cybersecurity-related incident is reported, the incident response team takes charge of the incident and matrixes in appropriate resources from elsewhere in IT and the organization to investigate and remediate the situation. Matrixing in external support may also be needed due to required expertise and knowledge, or workload constraints on the available incident response personnel.

Required activities for this functional area include the following:
- Ensure that the incident response team tracks cybersecurity threats against the organization and informs cybersecurity and IT leadership of threats posing new or previously unknown risks to the organization, as well as potential mitigations for those risks.
- Ensure that all information systems supporting organization business processes have a documented incident response process. Clearly define incident response process roles and responsibilities. Include, as appropriate, shared services for incident response that are centrally operated by cybersecurity.
- Designate a single leader for major incidents for the duration of the incident, from initiation to conclusion. Assign the following responsibilities to the leader:
  - Coordinate containment of the incident.
  - Reduce the operational impact of the incident.
  - Ensure remediation of compromised computers, accounts, or network traffic/protocols.
  - Keep stakeholders informed of incident response status.
- Investigate suspected incidents according to the following time frames:
  - "Critical" alerts: within one hour of their detection.

  - "High" alerts: within 12 hours of their detection.
  - "Medium" alerts: within 24 hours of their occurrence.
  - "Low" or "routine" alerts: within two business days of their occurrence.
- Document all incidents to capture the originating alert or event, investigation results, remediation, and conclusion. Investigate, identify, and document root causes of confirmed incidents. Retain incident documentation for seven years following the conclusion of the incident.
- Ensure incident investigation teams have the tools and permissions they need to investigate accounts, computers, and networks involved in malicious activity. Ensure teams have the ability to – either directly or by request – disable and remediate accounts, computers, and networks as necessary to contain and resolve the incident.
- Assign the cybersecurity department the following responsibilities:
  - Identification of incidents with contractual, regulatory, or legal implications.
  - Oversight and reporting of contractual, regulatory, or legal obligations related to incidents.
  - Application of the appropriate resources to ensure that contractual, regulatory, and legal obligations related to incidents are met.
- Enable anonymous methods for employees to report security policy violations or suspected security incidents without fear of reprisal.

Within this functional area, mandatory review, validation, testing, and training activities include the following:

- Review incident response security configurations – including re-validation of all policy exceptions – on an annual basis.
- Review the incidents that occurred and recommend strategic changes to the organization's cybersecurity policies and controls, on an annual basis.
- Verify and test incident response preventive, detective, audit, and forensic controls for proper operation at least annually.

Appendix D
Online Cybersecurity Resources

The online cyber resources listed in this appendix are a selected compilation of references that can help provide insight into various security awareness issues and training programs. *The short descriptions provided are quoted or significantly paraphrased from the resources.*

This resource list is not exhaustive. Most of the entries are resources that the authors reviewed during the preparation of this book, but their review does not constitute their endorsement. These resources are mostly US-based, but generally apply worldwide.

1. American Association of Retired Persons (AARP) Fraud Watch Network

- https://www.aarp.org/money/scams-fraud/

This website provides information to help the user "learn how to spot and avoid common scams." The site provides a Fraud Resource Center that lists scams and frauds including the following:

- Charity Scams
- Cryptocurrency Fraud
- Debt Collection Scams
- Government Grant Scams
- Health Insurance Scams
- Identity Theft
- Investment Fraud
- Online Pharmacy Scams
- Robocalls
- Tax ID Theft

Each scam or fraud is briefly described, along with a list of warning signs (for example, the pressure to close the deal immediately). The explanation provides the user with a list of *Do's* and *Don'ts* to help avoid becoming a victim.

2. American Association of Retired Persons (AARP) Scam Tracking Map

- https://www.aarp.org/money/scams-fraud/tracking-map.html

"No matter where you live, fraud is never far away. But you can protect yourself by knowing what to watch out for—and by telling others when you've

https://doi.org/10.1515/9781501506529-018

spotted a scam. Search the map to learn more about scams reported by people just like you. And use the pull-down menu to read law enforcement alerts."

This website provides short descriptions of scams reported by people within the United States by state, including the date that the scam was reported. The user can retrieve the scam descriptions by selecting a specific state and then clicking on an interactive map that displays the scams located within the state. Users are encouraged to report the scams they have heard of, to help warn others.

3. American Council for Technology and Industry Advisory Council (ACT-IAC)

- https://www.actiac.org/

The American Council for Technology and Industry Advisory Council (ACT-IAC) is a 501(c)(3) non-profit educational organization established to improve the government through the effective and innovative application of technology. ACT-IAC provides an objective, trusted, and ethical forum where government and industry executives can communicate, collaborate, and learn. ACT-IAC is the premier public-private partnership in the government technology community and has been called "*an example of how government and industry can work together*."

4. Cyber Security

- https://www.henrystewartpublications.com/csj

"*Cyber Security* is the major peer-reviewed journal publishing in-depth articles and case studies written by and for cyber security professionals. It showcases the latest thinking and best practices in cyber security, cyber resilience, cybercrime and cyber warfare, drawing on practical experience in national critical infrastructure, government, corporate, finance, military and not-for-profit sectors."

5. Cybersecurity Information Forum at George Mason University

- https://care.gmu.edu/cybersecurity-innovation-forum/

"Cybersecurity Innovation Forum at George Mason University is a local Meetup group sponsored by CARE [Center for Assurance Research and Engineering] and the School of Business. The group meets several times a year and features a series of 15-minute case study presentations by cybersecurity experts and technology innovators, followed by a panel discussion and questions. The focus of the meetings is on cybersecurity innovation, including innovation rationale and motivation, technology, metrics, and lessons learned."

6. Department of Homeland Security, National Initiative for Cybersecurity Careers and Studies

- https://niccs.us-cert.gov/national-cybersecurity-awareness-month-2019

"Held every October, National Cybersecurity Awareness Month (NCSAM) is a collaborative effort between government and industry to raise awareness about the importance of cybersecurity and to ensure that all Americans have the resources they need to be safer and more secure online."

7. Department of Justice, Bureau of Justice Statistics (BJS)

- https://www.bjs.gov/

The Bureau of Justice Statistics (BJS) is the primary source of criminal justice statistics for the United States. The BJS mission is "to collect, analyze, publish, and disseminate information on crime, criminal offenders, victims of crime, and the operation of justice systems at all levels of government."

8. Electronic Protected Health Information (ePHI) Security Risk Assessment Tool

- https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment

This Security Risk Assessment Tool is designed "to help healthcare providers conduct a security risk assessment as required by the HIPAA Security Rule and the Centers for Medicare and Medicaid Service (CMS) Electronic Health Record (EHR) Incentive Program." This tool helps a user identify and assess the risk to electronic public health information (ePHI) in the user's practice so that the user can implement appropriate safeguards.

9. General Data Protection Regulations (GDPR) Compliance GDPR, Article 4 GDPR Definitions

- https://gdpr.eu/
- https://gdpr.eu/article-4-definitions/

"GDPR.eu is a resource for organizations and individuals researching the General Data Protection Regulation. Here you'll find a library of straightforward and up-to-date information to help organizations achieve GDPR compliance."

10. Global Information Assurance Certification (GIAC)

- https://www.giac.org/

GIAC provides a set of vendor-neutral computer security certifications linked to the training courses provided by the SysAdmin, Audit, Network and Security (SANS) Institute. GIAC is specific to the leading-edge technological advancement of IT security in order to keep ahead of "black hat" techniques.

11. Health Industry Cybersecurity Practices (HICP)

- https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx

"*Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients* (HICP), the primary publication of the Cybersecurity Act of 2015, Section 405(d) Task Group, aims to raise awareness, provide vetted cybersecurity practices, and move organizations toward consistency in mitigating the current most pertinent cybersecurity threats to the sector.

The HICP examines cybersecurity threats and vulnerabilities that affect the healthcare industry. It explores (5) current threats, presents (10) practices to mitigate those threats, and includes a variety of cybersecurity resources and templates for end users to reference."

12. InfoSec Institute – Technology Training Company

- https://www.infosecinstitute.com/
- https://resources.infosecinstitute.com/category/certifications-training/

"InfoSec Institute is a technology training company. It provides certification-based training courses for security professionals and enterprise-grade security awareness and phishing training for businesses, agencies, and technology professionals.

. . . 2,000+ security awareness resources and phishing simulations help you change behavior and culture . . .

. . . over 50 certification learning paths and 325+ courses **mapped** [emphasis added] to the National Initiative for Cybersecurity Education's [NICE] CyberSeek model . . .

. . . boot camps designed to help you pass your certification exam."

13. International Journal of Cyber-Security and Digital Forensics (IJCSDF)

– http://sdiwc.net/ijcsdf/

"*The International Journal of Cyber-Security and Digital Forensics* (IJCSDF) is a knowledge resource for practitioners, scientists, and researchers among others working in various fields of Cyber Security, Privacy, Trust, Digital Forensics, Hacking, and Cyber Warfare. We welcome original contributions as high-quality technical papers (full and short) describing original unpublished results of theoretical, empirical, conceptual or experimental research.

IJCSDF is an open access journal which means that all content is freely available without charge to the user or his/her institution. Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the articles in this journal without asking prior permission from the publisher or the author.

The IJCSDF scope covers the following areas (but not limited to): cyber security, computer forensics, privacy, trust, hacking techniques, cyber warfare, cryptography, cybercrime, cyber-terrorism, cryptography, formal methods application in security and forensics, data piracy, database security and forensics, wired and wireless network security and investigation, mobile network security and forensics, incident handling, malware forensics and steganography."

14. Journal of Cybersecurity

– https://academic.oup.com/cybersecurity

"*Journal of Cybersecurity* publishes accessible articles describing original research in the inherently interdisciplinary cyber domain. *Journal of Cybersecurity* is premised on the belief that computer science-based approaches, while necessary, are not sufficient to tackle cybersecurity challenges. Instead, scholarly contributions from a range of disciplines are needed to understand the varied aspects of cybersecurity."

15. National Centers of Academic Excellence

– https://www.nsa.gov/resources/students-educators/centers-academic-excellence/

The U.S. National Security Agency (NSA) sponsors the following two Centers of Academic Excellence (CAE):

– ***Cyber Defense.*** "The goal of the program is to reduce vulnerability in our national information infrastructure by promoting higher education and research in cyber defense and producing professionals with cyber defense expertise."

- ***Cyber Operations.*** The program "supports the President's National Initiative for Cybersecurity Education (NICE): Building a Digital Nation, and furthers the goal to broaden the pool of skilled workers capable of supporting a cyber-secure nation."

16. National Cyber Security Alliance

- https://staysafeonline.org/

"Stay Safe Online, the National Cyber Security Alliance's website, aims to make the internet safer and more security for everyone.

The National Cyber Security Alliance, a 501(c)(3) non-profit founded in 2001, is a public private partnership, working with the Department of Homeland Security, private sector sponsors, and nonprofit collaborators to promote cyber security awareness for home users, small and medium size businesses, and primary and secondary education."

17. National Cybersecurity Center of Excellence (NCCoE)

- https://www.nccoe.nist.gov/

"The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges."

18. National Institute for Standards and Technology (NIST), Contingency Planning Guide for Federal Information Systems

- https://csrc.nist.gov/Topics/Security-and-Privacy/security-programs-and-operations/contingency-planning
- https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final

"Information system contingency planning refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of information systems, operations, and data after a disruption."

19. National Institute for Standards and Technology (NIST), Information Technology Laboratory, Computer Security Resource Center (CSRC)

- https://csrc.nist.gov/
- https://csrc.nist.gov/publications/sp800

"For 20 years, the Computer Security Resource Center (CSRC) has provided access to NIST's cybersecurity- and information security-related projects, publications, news, and events. CSRC supports stakeholders in government, industry, and academia—both in the U.S. and internationally."

20. National Institute for Standards and Technology (NIST), National Initiative for Cybersecurity Education (NICE)

- https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

"The NICE Framework, NIST Special Publication 800-181, is a national focused resource that categorizes and describes cybersecurity work. The NICE Framework establishes a taxonomy and common lexicon that describes cybersecurity work and workers irrespective of where or for whom the work is performed. The NICE Framework is intended to be applied in the public, private, and academic sectors.

The Executive Order (EO) on America's Cybersecurity Workforce encourages widespread adoption of the NICE Framework, and highlights its voluntary integration into existing education, training, and workforce development efforts undertaken by State, territorial, local, tribal, academic, non-profit, and private-sector entities.

The NICE Framework is comprised of the following three major components:

- Categories (7) – A high-level grouping of common cybersecurity functions.
- Specialty Areas (33) – Distinct areas of cybersecurity work.
- Work Roles (52) – The most detailed groupings of cybersecurity work comprised of specific knowledge, skills, and abilities required to perform tasks in a work role."

Table D.1 illustrates the NICE Framework *workforce categories* in terms of *specialty areas* and *work roles*. The NICE Framework "serves as a fundamental reference resource for describing and sharing information about cybersecurity work and the knowledge, skills, and abilities (KSAs) needed to complete tasks that can strengthen the cybersecurity posture of an organization."

The NICE Framework provides "a common, consistent lexicon that categorizes and describes cybersecurity work" and helps to improve "communication about how to identify, recruit, develop, and retain cybersecurity talent."

Table D.1: The NICE Cybersecurity Framework delineates workforce categories, corresponding specialty areas, and specific work roles.

Workforce Categories	Specialty Areas	Work Roles
Securely Provision (SP)	Risk Management (RSK)	– Authorizing Official/Designating Representative – Security Control Assessor
	Software Development (DEV)	– Software Developer – Secure Software Assessor
	Systems Architecture (ARC)	– Enterprise Architect – Security Architect
	Technology R&D (TRD)	– Research and Development Specialist
	Systems Requirements Planning (SRP)	– Systems Requirements Planner
	Test and Evaluation (TST)	– Systems Testing and Evaluation Specialist
	Systems Development (SYS)	– Information Systems Security Developer – Systems Developer
Operate and Maintain (OM)	Data Administration (DTA)	– Database Administrator – Data Analyst
	Knowledge Management (KMG)	– Knowledge Manager
	Customer Service and Technical Support (STS)	– Technical Support Specialist
	Network Services (NET)	– Network Operations Specialist
	Systems Administration (ADM)	– Systems Administrator
	Systems Analysis (ANA)	– Systems Security Analyst

Table D.1 (continued)

Workforce Categories	Specialty Areas	Work Roles
Oversee and Govern (OV)	Legal Advice and Advocacy (LGA)	– Cyber Legal Advisor – Privacy Officer/Privacy Compliance Manager
	Training, Education, and Awareness (TEA)	– Cyber Instructional Curriculum Developer – Cyber Instructor
	Cybersecurity Management (MGT)	– Information Systems Security Manager – Communications Security (COMSEC) Manager
	Strategic Planning and Policy (SPP)	– Cyber Workforce Developer and Manager – Cyber Policy and Strategy Planner
	Executive Cyber Leadership (EXL)	– Executive Cyber Leadership
	Program/Project Management (PMA) and Acquisition	– Program Manager – IT Project Manager – Product Support Manager – IT Investment/Portfolio Manager – IT Program Auditor
Protect and Defend (PR)	Cyber Defense Analysis (CDA)	– Cyber Defense Analyst
	Cyber Defense Infrastructure Support (INF)	– Cyber Defense Infrastructure Support Specialist
	Incident Response (IR)	– Cyber Defense Incident Responder
	Vulnerability Assessment and Management (VAM)	– Vulnerability Assessment Analyst
Analyze (AN)	Threat Analysis (TWA)	– Threat/Warning Analyst
	Exploitation Analysis (EXP)	– Exploitation Analyst
	All-Source Analysis (ASA)	– All-Source Analyst – Mission Assessment Specialist
	Targets (TGT)	– Target Developer – Target Network Analyst
	Language Analysis (LNG)	– Multi-Disciplined Language Analyst

Table D.1 (continued)

Workforce Categories	Specialty Areas	Work Roles
Collect and Operate (CO)	Collection Operations (CLO)	– All-Source Collection Manager – All-Source Collection Requirements Manager
	Cyber Operational Planning (OPL)	– Cyber Intel Planner – Cyber Ops Planner – Partner Integration Planner
	Cyber Operations (OPS)	– Cyber Operator
Investigate (IN)	Cyber Investigation (INV)	– Cyber Crime Investigator
	Digital Forensics (FOR)	– Law Enforce/Counter Intel Forensics Analyst – Cyber Defense Forensics Analyst

Organizations can use the NICE Framework "to develop additional publications or tools that meet their needs to define or provide guidance on different aspects of cybersecurity workforce development, planning, training, and education."

21. No More Ransom

– https://www.nomoreransom.org/en/decryption-tools.html

This website checks files to help identify the type of ransomware affecting a particular device and to help determine whether there is a solution available to decrypt the device.

This website is "an initiative by the National High-Tech Crime Unit of the Netherlands' police, Europol's European Cybercrime Centre, and McAfee with the goal to help victims of ransomware retrieve their encrypted data without having to pay the criminals.

Since it is much easier to avoid the threat than to fight against it once the system is affected, the project also aims to educate users about how ransomware works and what countermeasures can be taken to effectively prevent infection. The more parties supporting this project, the better the results can be. This initiative is open to other public and private parties."

22. Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)), Cybersecurity Maturity Model Certification

- https://www.acq.osd.mil/cmmc/
- https://www.acq.osd.mil/cmmc/docs/CMMC_Model_Appendices_20200203.pdf

"The Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD[A&S]) recognizes that security is foundational to acquisition and should not be traded along with cost, schedule, and performance moving forward. The Department is committed to working with the Defense Industrial Base (DIB) sector to enhance the protection of controlled unclassified information (CUI) within the supply chain.

OUSD(A&S) is working with DoD stakeholders, University Affiliated Research Centers (UARCs), Federally Funded Research and Development Centers (FFRDC), and industry to develop the Cybersecurity Maturity Model Certification (CMMC)."

23. Open Web Application Security Project™ (OWASP)

- https://www.owasp.org/index.php/Main_Page

OWASP is an "unbiased source of information" on application security (AppSec) software practices and tools, as well as an active body advocating open standards. OWASP provides "impartial, practical information about AppSec to individuals, corporations, universities, government agencies, and other organizations worldwide."

24. Publications Office of the European Union

- https://op.europa.eu/en/home

"The Publications Office of the European Union (Publications Office), based in Luxembourg, is an interinstitutional office whose task is to publish the publications of the institutions of the European Union (Decision 2009/496/EC, Euratom). Its core activities include production and dissemination of legal and general publications in a variety of paper and electronic formats, managing a range of websites providing EU citizens, governments, and businesses with digital access to official information and data from the EU, including EUR-Lex, the EU Open Data Portal, EU Publications, TED (Tenders Electronic Daily), CORDIS, and ensuring long-term preservation of content produced by EU institutions and bodies."

25. SysAdmin, Audit, Network, and Security (SANS) Institute

- https://www.sans.org/about/

The SANS Institute is a cooperative research and education organization that reaches "more than 165,000 security professionals around the world" and is the "most trusted and by far the largest source for information security training in the world."

SANS "develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system—the Internet Storm Center."

SANS "offers training through several delivery methods—live and virtual, classroom-style, online at your own pace or webcast with live instruction, guided study with a local mentor, or privately at your workplace where even your most remote colleagues can join in via Simulcast."

SANS "offers certification via GIAC [Global Information Assurance Certification], an affiliate of the SANS Institute featuring over 35 hands-on, technical information security certifications in information security, a Master's Degree program through SANS Technology Institute graduate school, as well as numerous free security resources including newsletters, whitepapers, and webcasts."

26. U.S. National Vulnerability Database (NVD)

- https://nvd.nist.gov/
- https://csrc.nist.gov/projects/security-content-automation-protocol/
- https://csrc.nist.gov/Projects/National-Checklist-Program

"The NVD is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics."

"The Security Content Automation Protocol (SCAP) is a synthesis of interoperable specifications derived from community ideas. Community participation is a great strength for SCAP, because the security automation community ensures the broadest possible range of use cases is reflected in SCAP functionality."

"NIST maintains the National Checklist Repository, which is a publicly available resource that contains information on a variety of security configuration checklists for specific IT products or categories of IT products. A security configuration checklist (also called a lockdown, hardening guide, or benchmark) is a series of instructions or procedures for configuring an IT product to a particular

operational environment, for verifying that the product has been configured properly, and/or for identifying unauthorized changes to the product. The IT product may be commercial, open source, government-off-the-shelf (GOTS), etc."

"The National Checklist Program (NCP), defined by the NIST SP 800-70, is the U.S. government repository of publicly available security checklists (or benchmarks) that provide detailed low-level guidance on setting the security configuration of operating systems and applications."

27. Veracode

- https://www.veracode.com/about
- https://www.veracode.com/blog/secure-development/give-developers-training-actually-helps

Veracode is an application security company that "provides an automated cloud-based service for securing web, mobile and third-party enterprise applications. Veracode provides multiple security analysis technologies on a single platform, including static analysis, dynamic analysis, mobile application behavioral analysis and software composition analysis."

28. *Wall Street Journal* Pro's Cybersecurity

- https://cyber.wsj.com/
- https://cyber.wsj.com/small-business-academy/

This website provides "actionable cybersecurity insight" through "a series of live journalism events, our news, commentary, and training." The website also provides access to the Small Business Academy consisting, in part, of a series of events to connect people with peers, experts, and cybersecurity practitioners.

Glossary

This glossary contains definitions of many terms used in this book. Terms that are used in definitions and are defined elsewhere in the glossary are italicized.[1]

A

Advanced Persistent Threat (APT) – An advanced cyberattacker who penetrates a victim's network and maintains persistence within that environment to carry out cyberattacks over time. Uses advanced techniques to gain and retain access, particularly for conducting espionage or data theft.

Alert – A *cybersecurity event* that undoubtedly indicates *malicious* behavior and generates an alarm on a detection system. The alarm indicates that an *incident* is occurring and requires investigation or follow-up.

Assessments – *Cybersecurity control* assessments are used to give management feedback on where controls are strong or weak, usually organized according to an assessment framework such the National Institute for Standards and Technologies Cyber Security Framework (NIST CSF). The output of an assessment consists of observations and recommendations organized according to the framework, and is intended to give management inputs on where investments should be made and where controls should be improved.

Authentication – The process of uniquely identifying oneself to a computer. Authentication is generally performed using a username and a *password*, although *strong authentication* or *multifactor authentication* may also be used.

Audit – *Cybersecurity control* audits are usually performed to validate compliance with an external standard, like the Payment Card Industry Digital Security Standard (PCI-DSS) or the Health Insurance Portability and Accountability Act (HIPAA). The output of the audit is a "yes-no" result, along with accompanying evidence and artifacts to support that assertion.

Availability – One element of the *cyberdefense* triad of *confidentiality*, *integrity*, and availability (CIA). Availability refers to information technology services being available for use. An availability attack denies access to those services, usually through *denial-of-service* or *distributed denial-of-service* attacks.

B

Biometrics – A method of *strong authentication* that uses biological attributes such as fingerprints, iris patterns, or facial geometry to uniquely identify a person.

Blacklisting – A security method that involves identifying accounts, applications, networks, passwords, or network protocols that are explicitly untrusted. Accounts on a blacklist might not be permitted to log on. Applications on a blacklist might not be permitted to install or run. Network addresses or protocols on a blacklist might not be permitted to communicate. Blacklisting is in contrast to *whitelisting*.

---

1 Some material is adapted from Donaldson, Scott E., Williams, Chris K. and Siegel, Stanley G. *Understanding Security Issues*, Walter de Gruyter Inc., 2019.

https://doi.org/10.1515/9781501506529-019

Blockchain – Distributed digital ledgers containing data structures (i.e., blocks) that are cryptographically linked together (i.e., chains) and "distributed in a peer-to-peer network to prevent tampering of previously published transactions."[2]

Botnet – A network of *compromised* computers that are all under an attacker's central control. It can be used to conduct *distributed denial-of-service* attacks or to obtain initial entry to a victim's *enterprise* through compromised computers. Such attacks overload IT systems with a massive surge of network traffic, causing infrastructure servers to time out from a few seconds to a few hours.

Breach – The *compromise* of a system, networking resource, or data by an attacker who overcomes or defeats the established protection measures.

Brute Force Attack – A credential attack method that involves comprehensively trying all possible combinations of letters and numbers to try and deduce the correct *password*. This attack is often used to guess passwords or *encryption keys*. Websites and applications can counter brute force attacks by introducing a delay after each unsuccessful password attempt, by locking accounts after a certain number of unsuccessful login attempts, and by protecting encrypted credential databases from unauthorized access.

Bug Bounty Program – An arrangement where individuals can receive compensation for identifying and reporting "software bugs" (i.e., computer program errors) to organizations (e. g., Netflix, Starbucks, PayPal, Twitter).

C

CIA – The *cyberdefense* triad of *confidentiality*, *integrity*, and *availability*. *Cyberattacks* involve compromising one or more of these properties of information technology systems, and cyberdefenses involve protecting these properties.

Click Fraud – Cyberattackers can use compromised computers as if they belonged to the cyberattackers. Website owners post ads and are paid based on the number of website visitors who "click" on the ads. Attackers manipulate the compromised computers to "click on" such advertisements, generating revenue from advertisers who pay the attackers for illegitimate customer leads that the advertisers believe are legitimate.

Compromise – The act of taking control of an account, computer, *endpoint*, or *device* and modifying its configuration to suit the needs of the attacker. Frequently, compromise involves exploiting a *vulnerability* to install *malware* that gives the attacker some capability with regard to attacking the victim. In the case of accounts, compromise may involve the attacker obtaining knowledge of the victim's user account and password *credentials*.

Confidentiality – One element of the *cyberdefense* triad of confidentiality, *integrity*, and *availability* (CIA). Confidentiality refers to the protection of data that should not be disclosed to people not authorized to have access to the data.

---

2 Definition adapted from Yaga, Mell, Roby, Scarfone. "Blockchain Technology Overview," National Institute of Standards and Technology, Gaithersburg, MD, NIST Internal Report 8202 (NISTIR 8202). https://doi.org/10.6028/NIST.IR.8202.

Credential – A parameter for *authentication* consisting of a user identity (e.g., *username*) and a proof of identity such as a *password* or *multifactor authentication token*.

Cryptography – *Cybersecurity* practice that includes processes for generating numbers used to *encrypt* data so it cannot be read by an attacker, apply *digital signatures* to data to detect unauthorized changes, and deliver *strong authentication* to uniquely identify users and computers over the internet.

Cyberattack – An attack conducted using computers and information systems to *compromise* the *confidentiality*, *integrity*, and/or *availability* of the target's information and information systems.

Cyber Awareness – A mindset that involves thinking about how our daily actions affect our security posture at work, at home, and on travel. When we are cyber aware, we are continuously thinking about the security consequences of our actions. Organization cyber awareness involves thinking about how the interwoven activities of personnel, customers, partners, service providers, and vendors can affect an organization's security posture.

Cybercrime – Cybercrime is criminal activity involving the internet, dark web, and using hacking or malware to exploit victims' computers, networks, accounts, and sensitive data.

Cyberdefense – The act of defending computers and information systems from *cyberattacks*.

Cybersecurity – The practice of protecting the *confidentiality*, *integrity*, and *availability* of IT assets from *cyberattacks* using *cyberdefense* techniques.

Cybersecurity Capability – A process or technology that enables the organization to perform a specific *cybersecurity control*. Cybersecurity capability is further defined as providing for auditing, logging, detection, or prevention of a particular type of malicious behavior.

Cybersecurity Control – A means of enforcing a security policy within the *enterprise*. A control is a way of providing some level of assurance that a type of undesirable behavior (i.e., cybersecurity risk) is or is not occurring within the enterprise. Controls can be of multiple types, including the following: (1) preventive controls that prevent undesired behaviors, (2) detective controls that detect undesired behaviors, (3) *forensic* controls that log undesired behaviors so they can be investigated afterward, and (4) *audit* controls that search for undesired behaviors, (5) response controls that enable the organization to take action against a *cyberattack*, and (6) recovery controls that enable the organization to resume normal operations after a *cyberattack*. Each control type has advantages, disadvantages, costs, and trade-offs.

D

Denial of Service (DoS) – A *cyberattack* method that involves disabling IT systems either temporarily or permanently, thereby denying their *availability* to the intended users.

Device – A network-connected component that has computing capabilities but is not normally called a computer. Common devices include mobile phones, tablets, network-connected sensors, personal assistants, network-enabled home appliances, digital media players, and computing accessories such as printers or cameras.

DevOps – A software engineering practice designed to integrate development (i.e., software developers) and operations (i.e., IT infrastructure professionals) teams to achieve rapid development cycles that frequently and reliably deliver software products, features, and services to customers. DevOps typically requires an integrated set of software tools designed to coordinate an automated release process throughout the entire software development life cycle (e.g., requirements, design, development, testing, deployment, operate, retirement).

DevSecOps – Similar to *DevOps* with respect to rapid development cycles, frequent and reliable software applications to customers, but with the addition of security "built in" to applications rather than "bolted on" after the applications are released. DevSecOps promotes a philosophy that security is everyone's responsibility, versus a centralized security decision-making authority.

Digital Signature – A *cryptographic* technique for protecting the *integrity* of data by calculating a *hash* of the data and then cryptographically processing the *hash* through an industry-trusted (i.e., industry-certified) algorithm. This technique makes it possible to prove the authenticity of the data, detect unauthorized changes, and achieve *non-repudiation* of people using the systems.

Distributed Denial of Service (DDoS) – A *denial-of-service* attack that uses a distributed network—usually a *botnet*—to overload IT systems with a massive surge of network traffic that the victim's IT infrastructure is unable to handle.

E

Encryption – A *cryptographic* technique for protecting data so it can only be read by holders of the legitimate *key*. Encryption effectiveness is dependent on the strength of the algorithms and keys used, the creation of truly random key number sequences, management of encryption keys over their life cycles, and numerous other technical factors.

Endpoint – Any type of computing system, including servers, personal computers, appliances, mobile *devices* such as smartphones, or other network-connected *devices*. Endpoints are subject to security policies and capabilities intended to prevent their *compromise*.

Enterprise – An organization that uses computers or computer networks for personal, business, and country (i.e., nation-state) purposes. An enterprise has authority over the computers and computer networks within its domain. An enterprise may range from an individual's personal computer and home network up to a corporate or governmental entity with thousands or hundreds of thousands of computers connected to networks spanning the globe.

Escalate Privileges – In a *cyberattack*, attackers obtain additional privileges in the *enterprise*. For example, going from regular user to *systems administrator* status on a personal computer or file server, or escalating from computer administrator to network administrator status on an enterprise network.

Espionage – The act of clandestinely acquiring sensitive, confidential, or secret information without consent of the entity—government, organization, individual—that has such information. Governments conduct espionage, in part, for political, military, or economic reasons. Organizations conduct espionage, in part, to obtain competitor trade secrets, intellectual property, financial information, and planning documentation.

Event – An incidence of behavior that is identified by a detective *cybersecurity control* and may be an indication of *malicious* behavior. *Incidents* are generated when one or more events together constitute an *indicator of compromise* and warrant investigation.

F

Firewall – A hardware or software security capability that connects to a network and applies a security *policy* to determine what network traffic is allowed to pass and what network traffic is blocked. It can also *alert* on certain types of network traffic that might indicate an attack.

Forensics – The science of investigating *compromised* computer systems to understand attacker *tools, techniques, and procedures*, and to determine *indicators of compromise*. Forensic investigation involves analyzing logs, files, and sometimes program code to understand attacker activities and methods.

Functional Areas – Comprised of *cybersecurity capabilities* that deliver *cybersecurity controls* that are used to protect core organizational IT systems, sensitive data, and business functions.

G

Gold Code – A configuration-managed version of software code that is generally used as a master image for software code installation on multiple computers. Gold code usually applies to operating system images and configurations, or application software builds that are approved for release or distribution.

H

Hackers – A person who obtains unauthorized access to computer systems, usually by exploiting *vulnerabilities* in computer systems security.

Hacking – The act of obtaining unauthorized access to computer systems, usually by exploiting *vulnerabilities* in computer systems security. People who perform these acts are called *hackers*.

Hardware Security Module (HSM) – A *cryptographic device* used to protect cryptographic *keys* from theft. Some models can also accelerate cryptographic operations such as *encryption*, decryption, or *digital signatures*.

Hash – A fixed-length *cryptographic* code calculated from a document or data field such that any change to the document or data field results in the hash changing as well. The algorithm is one-way, so knowledge of the hash does not lead to the original document or data being revealed. This capability is used to protect the *integrity* of documents from modification, as well as for *authentication* so that *passwords* do not need to be stored in a readable form.

I

Incident – A *cybersecurity* activity initiated by one or more *events* or *alerts* that indicate *malicious* behavior and warrant investigation according to an *incident response* process. Incidents are investigated using *security information and event management* systems, and

may utilize computer *forensics* to identify the attackers' *indicators of compromise* and *tools, techniques, and procedures*.

Incident Response – The practice of investigating, containing, remediating, resolving, and documenting *cybersecurity incidents* using *indicators of compromise* and performing *forensics* on *compromised* systems.

Indicators of Compromise (IOCs) – Indicators that can be used to identify attacker *malicious* activity in the *enterprise*. Indicators are usually accounts, computers, network addresses, or communications patterns that are identified using *forensics* and then used to generate additional *alerts* to identify *cyberattack* activity wherever it is occurring.

Integrity – One element of the *cyberdefense* triad of *confidentiality*, integrity, and *availability* (CIA). Integrity refers to having confidence that data is not changed by unauthorized people from when it is input into a computer system until it is later retrieved from the computer system. Integrity is particularly important for financial records, medical records, and transactions, but it can also apply to system configurations and other aspects of IT systems. Integrity attacks involve changing data or configurations through unauthorized means.

J, K

Keys – In *cryptography*, digital strings that are used to *encrypt*, decrypt (i.e., convert encrypted information back into plain language), and *digitally sign* data.

L

Lateral Movement – In a *cyberattack*, moving from one computer to another where both machines are at equivalent levels of *privilege*, or using *credentials* at a single privilege level. Lateral movement is in contrast with *escalating privileges*, where attackers obtain additional privileges within the victim environment.

M

Malicious – Adjective applied to behavior, network traffic, or software intended to *compromise* the *confidentiality*, *integrity*, or *availability* of *enterprise* data and IT systems.

Malware – *Malicious* software. Malware is generally characterized by one or more of the following properties: (1) it attempts to stay hidden or to persist on the victim computer after attempts to remove it, (2) it attempts to propagate from one victim computer to another, using *lateral movement*, (3) it collects data from the victim computer and sends it to another computer, (4) it collects user *credentials* for resources and/or websites, or (5) it *monitors* user behavior without the user's knowledge or consent.

Mitigation – In cybersecurity, the process of compensating for *risks*, *vulnerabilities*, or *threats* by reducing either the likelihood of their occurrence or the impact of their exploitation.

Mobile Device Management (MDM) – *Cybersecurity* technology for managing organization data stored on mobile *devices*. This technology generally works by either controlling the device itself or by creating within the device a protected data store or container for organization data. If the device is lost or stolen, this technology usually provides the ability to

erase the organization data (or even the entire device) so that organization data is not compromised.

Monitoring – Collecting and storing data, *events*, or *alerts* so they can be consolidated into one location for correlation and analysis in a *security information and event management* system. Monitoring can be for operational purposes to ensure that systems are performing properly, or for *cybersecurity* purposes to detect *incidents*.

Multifactor Authentication (MFA) – *Authentication* that relies on multiple factors of identity, usually something the user knows (such as a *password*) plus something the user has (such as a *token* or mobile *device*), or possibly a *biometric* (such as a fingerprint). Also known as *two-factor authentication* or *strong authentication*.

N

Non-Repudiation – Electronic proof of identity. Generally, non-repudiation is performed *cryptographically* by *digitally signing* a unique piece of data using a *key* that is only held by the party, thus providing the party's identity online.

Non-Credentialed Scanning – This type of scanning does not use system *credentials* to provide a vulnerability assessment from a cyberattacker's viewpoint. Credentialed scanning uses system *credentials* to provide a vulnerability assessment from an organization's viewpoint, which can include a list of required patches and misconfigurations.

O

One-Time Password – A *password* that is only used for a single *authentication* attempt.

Open Source Tools – Software tools that are developed by a user community and are available without commercial software product licenses, versus software tools developed by a software organization that issues commercial software product licenses for a profit.

P

Password – A string of characters known only to the user and used to *authenticate*. Knowledge of the password proves the user's identity to a computer system, provided the password has not been *compromised*.

Password Spraying – This attack uses a few commonly used *passwords* (e.g., password) to gain unauthorized access to a large number of accounts. Password spraying tries a common *password* against many accounts before using a second common *password* against those accounts. This technique is based on the knowledge that many users use common, low-security *passwords* like "password" or "12345." By contrast, *brute force attacks* try all possible combinations of letters and numbers to try and deduce the correct *password* for a single target account. *Password* spaying is designed to avoid the targeted account getting locked out due to security policies limiting the number of failed log-in attempts during a period of time.

Patch – A software or configuration update that addresses a performance or security issue that is distributed and installed after a system is in production. Installing the patch frequently involves a brief outage while the old software is stopped and the system is restarted running the new software.

Phishing – A *cyberattack* technique for obtaining initial entry to an organization that involves sending *malicious* e-mails to people using an organization's e-mail system. Phishing e-mails generally work by exploiting a *vulnerability* to install *malware* onto the victim's computer, by tricking the victim into installing the malware by himself or herself, or by tricking the victim into divulging his or her log-on *credentials* or *password*.

Policy – In cybersecurity, a management statement of behavior to be performed within the *enterprise*. An effective policy must have four properties: (1) it must be written, (2) it must be promulgated so people are aware of it, (3) it must include consequences for non-compliance, and (4) those consequences must be enforced as fairly, completely, and ethically as possible. In addition, policies are applied to specific security technologies, like firewalls, to identify which behaviors are to be permitted and which are to be blocked.

Privilege – A permission for access to an *enterprise* computer resource. Attackers frequently seek to *escalate privileges* to obtain administrative access to computer system and data through systems administrator accounts and *credentials*. With the appropriate administrator privileges, attackers can access and modify data at will.

Programmable Logic Array – This device is like a miniature computer that can be programmed to process sensor data and direct operation of physical systems like plant machinery. Unlike general-purpose computers, they do not usually run operating systems or have user interfaces. Attackers can change their programming and cause the machines they control to malfunction.

Q, R

Rainbow Tables – Rainbow tables are huge tables containing millions of data entries that can be used to try to guess a user's *password*. There are also password lookup tables containing millions of common password strings. These tables generally include all the words in the dictionary, along with common character substitutions within those words (e.g., adding a number to the end or replacing the letter "a" with the "@" symbol).

Ransomware – A form of *malware* that *encrypts* the data stored on the victim's computer and then demands a ransom to decrypt the data. If the user refuses the ransom, the *encryption key* is destroyed and the data is lost. More sophisticated ransomware versions are aware of backups, databases, file shares, and cloud storage. Such ransomware versions try to ensure that all copies of the data are encrypted and held ransom.

Recovery Point Objective (RPO) – RPO is the point in time that data is recovered through. For example, if the recovery point is nightly, then a recovery will not include transactions from the following day. Recovery point is about how up-to-date recovered data needs to be.

Recovery Time Objective (RTO) – RTO is how long it takes from when the disaster is declared until the system can be recovered and its data and transaction processing capabilities are available again.

Risk – In *cybersecurity*, the possibility that an attacker or *threat* interferes with the *confidentiality*, *integrity*, or *availability* of data or IT services. Normally, risk is analyzed based upon *threats* exploiting present *vulnerabilities* to cause an impact to the data or IT services.

S

Security Information and Event Management (SIEM) – Technology for collecting and matching *cybersecurity events* and *alerts*, as well as investigating and tracking *incidents* arising from them, as part of the *incident response* process.

Security Technical Implementation Guide (STIG) – A security configuration document, generally for operating system initial installations. The STIG specifies which operating system security features are to be enabled or disabled in an appropriately secure configuration.

Smart Card – A single-chip *hardware security module* contained in a credit card form factor that protects user *keys* for *authentication*, *encryption*, *digital signature*, and sometimes payment.

Spear Phishing – A *cyberattack* technique that involves sending highly targeted *phishing* e-mails to victims within an organization. Spear phishing e-mails may be created, in part, by using insider information, such as the names and roles of people of interest to the targeted victims.

Strong Authentication – *Authentication* that relies on multiple factors of identity, usually something the user knows (such as a *password*) plus something the user has (such as a *token* or mobile *device*), or possibly a *biometric* (such as a fingerprint). Also known as *multifactor authentication* or *two-factor authentication*.

Systems Administrator – An individual who administers a computer system. Generally, the systems administrator has *privileges* to be able to modify all data and software on the system, including applications and the operating systems. Many attacks attempt to *escalate privileges* to obtain systems administrator access to *enterprise* IT systems.

T

Threat – An entity—someone or something—that can exploit a *vulnerability* to pose a *risk* to the *enterprise* or its IT systems. A threat is motivated by some type of *malicious* intent against the *enterprise* and its IT systems.

Token – In *authentication*, a physical device used for *multifactor authentication*. Users prove that they are in possession of the token, usually by generating a *cryptographic* code from *keys* stored within it. Users then enter the *cryptographic* code into the computer, either by typing it in or through an electronic connection.

Tools, Techniques, and Procedures (TPPs) – In computer *forensics*, identification of how attackers are operating: (1) the applications and other tools they are using, (2) the techniques with which they are using those tools, and (3) the procedures they are following to perform those techniques. TTPs are important *indicators of compromise* used to track down attackers and repel them in an *incident response*.

Two-Factor Authentication – *Authentication* that relies on multiple factors of identify, usually something the user knows (such as a *password*) plus something the user has (such as a *token* or mobile *device*), or possibly a *biometric* (such as a fingerprint). Also known as *multifactor authentication* or *strong authentication*.

U

Username – A unique identification, such as a log-in name or e-mail address, associated with a specific user who is allowed access to *enterprise* applications or *endpoints* such as personal computers, mobile *devices*, or computer networks.

V

Virtual Private Network (VPN) – A network security technology that involves creating an *encrypted* tunnel from one host computer to another over an untrusted network. This encrypted tunnel is used to connect the networks at both ends so they are "virtually" connected and "private" from the network in between.

Virus – A form of *malware* that attaches itself to other pieces of software in order to propagate and run. A virus can be embedded into an application or computer operating system, but it is unable to run on its own. It usually includes the ability to replicate itself, and it may also have a payload to perform some type of destructive or *malicious* behavior.

Vulnerability – A flaw that allows a system to be exploited or *compromised* for *malicious* purposes by a cyber *threat* actor. Vulnerabilities may be flaws in computer hardware, software code, system configurations, or security architectures. Some vulnerabilities are remediated through *patches*, while others may require significant system redesign or technology replacement.

W

Whaling – A *cyberattack* technique that involves sending *spear phishing* e-mails to high-profile employees ("big phishes" or "whales") within an organization.

Whitelisting – A powerful *cybersecurity control* method that involves identifying accounts, applications, networks, or network protocols that are explicitly trusted. Whitelisting technology enforces that only those accounts, applications, networks, or network protocols on the approved list are permitted to operate. All other accounts, applications, networks, or network protocols are blocked and may generate *alerts* for investigation. Whitelisting is in contrast to *blacklisting*.

X, Y, Z

Zombie – A zombie account is an account that has been abandoned by its user and is no longer actively being used. However, because the account was never closed or de-provisioned, it may be taken over by attackers using large databases of compromised user credentials.

Zero-Day Exploit – A cyberattack that targets a *vulnerability* not publicly known and for which a patch is not yet available. Zero-day exploits are valuable to attackers because they can be difficult or impossible to block, the first time they are used. However, the use of a zero-day exploit can reveal the underlying *vulnerability* and give defenders the opportunity to mitigate the *vulnerability* through compensating *cybersecurity controls*, until a *patch* becomes available.

Zero-Trust Security – A security concept that operates on the principle of not trusting any user outside or inside the network perimeter, and requires that every user and computer be identified, *authenticated*, and granted specific *privileges* to access the rest of the *enterprise*. This is in contrast to traditional cybersecurity approaches that assume a level of trust to users and computers connected to the internal *enterprise* network, and may permit access and activities without further *authentication* or security checks.

Index

https://doi.org/10.1515/9781501506529-020