THE EXPERT'S VOICE® IN CYBERSECURITY

Enterprise Cybersecurity

How to Build a Successful Cyberdefense Program Against Advanced Threats

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

Apress®

For your convenience Apress has placed some of the front matter material after the index. Please use the Bookmarks and Contents at a Glance links to access them.

Apress®

Contents at a Glance

Introduction

Interest in cybersecurity is on the rise. As our world becomes more and more interconnected and more and more online, the damage cyberthreats can do to our cyberworld is increasing dramatically, day by day. For those of us old enough to remember life before personal computers—not to mention the Internet—it is staggering to consider how all of this connectivity has transformed our daily lives. Yet, as the online world developed in less than a generation, the ability to protect the online world has had even less time to develop and is still maturing.

Hardly a week goes by without an announcement of a cybersecurity breach or incident of some form or another, such as the following:

- Personal information compromised
- Credit cards stolen
- Medical records lost
- Companies hacked
- Governments targeted

The attackers perpetrating these crimes—and yes, most often these are criminal activities—seem to be acting with impunity compared to the defenders seeking to stop them. These hacks are occurring to major brand names, including Target, Home Depot, JP Morgan Chase, Sony, Apple, and many, many others. While many of the hacks hitting the headlines affect victims in the United States, the parties doing the hacking are in Russia, China, Korea, the Middle East, and elsewhere around the world. This problem is truly global.

If these hacks are happening to the biggest, most well-recognized and well-funded businesses and nations, then what chance do the *relatively smaller* cybertargets have at protecting themselves?

Anyone who is interested in cybersecurity or who is responsible for cybersecurity at an organization has certainly recognized that there is a long road ahead to achieving cybersecurity *success* against the threats mentioned here, however that success ends up being defined.

What Is This Book About?

This book is about achieving enterprise cybersecurity success. Does success mean computers never get compromised, malware never gets inside the enterprise, or breaches never occur? What success means depends on how an enterprise defines it. Cybersecurity professionals work with executive leadership to make business decisions on how *good* cybersecurity needs to be to defend the enterprise against cyberattackers. *Good* translates into various operational processes, cybersecurity capabilities, and information systems to protect the enterprise as needed to satisfy the business requirements.

Implementing a successful cyberdefense program against real-world attacks is what this book is about. Often in cybersecurity, everyone knows *what should be done*, but resources *to do it* are not sufficient. As shown in Figure I-1, the reality is that *the cybersecurity conundrum gets in the way of what needs to be done*. What cybersecurity professionals want to implement is more than what control frameworks specify, and it is far greater than what the budget allows. Ironically, another challenge is that even when defenders get everything they want, clever attackers are extremely effective at finding and exploiting the gaps in those defenses, regardless of their comprehensiveness. The challenge is to spend the available budget on the right protections so that real-world attacks can be thwarted without breaking the bank.

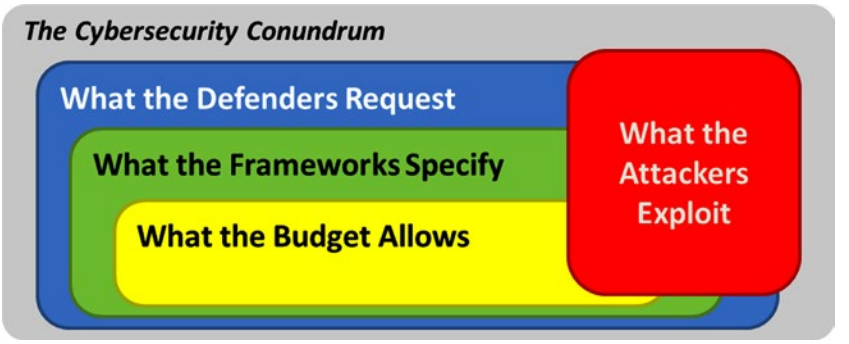

Figure I-1. *Even though the cybersecurity conundrum presents significant challenges, this book is about implementing a successful cyberdefense program that works against real-world attacks, despite the challenges.*

The cybersecurity business challenge is compounded by the fact that cyberthreats have to be looked at within the larger business context. The reality is cyberthreats are just one of *many* threats against the business and, from a budget perspective, are relatively small threats. Therefore, the enterprise has to prioritize limited resources to get the best possible security for the available budget.

Cybersecurity will *never* be funded to do everything that is desired, or even mandated by available *best practice* cybersecurity frameworks.

Cybersecurity professionals are frustrated, in part, because they request resources to fight threats that are, from a business perspective, a rounding error on the bottom line. In other words, the cyberbudget is a relatively small percentage of the organization's overall financial posture. Cybersecurity needs to be planned around the idea of achieving only partial security, rather than being resourced to do everything perfectly all the time.

Ironically, the major cybersecurity frameworks lay out what the *ideal* practices should be, but have little, if any, guidance on how to deploy a *partial* solution that is the best value for the cost when the funding is not adequate to achieve the ideal. Cybersecurity professionals must learn how to work with the business to find a new balance. Indeed, in a resource-constrained environment, cyberdefenders must consider how to build defenses that are only partially successful, but are wholly effective in the eyes of the business. This balance requires a new mindset, powered by the following axioms of cyberdefense:

Axioms of a "Next-Generation" Cyberdefense:

1. Assume an intelligent attacker will eventually defeat all defensive measures.
2. Design defenses to detect and delay attacks so that defenders have time to respond.
3. Layer defenses to contain attacks and provide redundancy in protection.
4. Use an active defense to catch and repel attacks after they start but before they can succeed.

With these axioms in mind, there is an acknowledged need for a framework that enables cybersecurity professionals to deploy balanced security with limited resources. Simply stated, cybersecurity professionals are not going to be able to implement the ideal solution.

This book presents a cybersecurity methodology for designing, managing, and operating a *balanced* enterprise cybersecurity program that is pragmatic and realistic in the face of resource constraints and other real-world limitations. In this book, the reader will learn the following:

- The methodology of targeted attacks and why they succeed
- The cybersecurity risk management process
- Why cybersecurity capabilities are the foundation of every successful cybersecurity program
- How to organize a cybersecurity program
- How to assess and score a cybersecurity program
- How to report cybersecurity program status against compliance and regulatory frameworks
- The operational processes and supporting information systems of a successful cybersecurity program
- How to create a data-driven and objectively managed cybersecurity program
- How cybersecurity is evolving and will continue to evolve over the next decade

Who Should Read This Book?

This book is for anyone interested in modern cybersecurity, as depicted by Figure I-2.

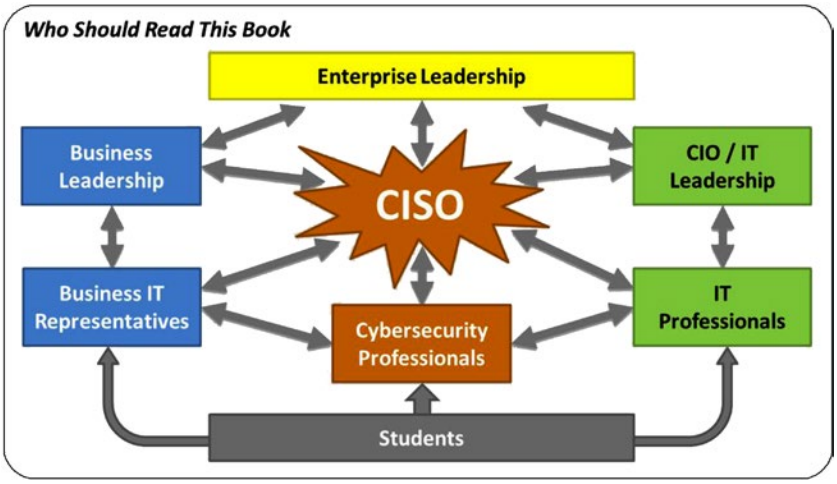

Figure I-2. *This book should be read by everyone involved in or interested in successful enterprise cybersecurity.*

Readers of this book include the following:

- ***Enterprise Leadership*** with oversight responsibility for information technology and cybersecurity concerns within an organization, business, or government agency.
- ***Chief Information Security Officer (CISO)*** or cybersecurity director who is responsible for overseeing a comprehensive cybersecurity program at his or her enterprise.
- ***Cybersecurity Professional*** who is responsible for managing, deploying, and operating effective cyberdefenses within the enterprise.
- ***Chief Information Officer (CIO)*** or ***Information Technology (IT) Leadership*** who are responsible for deploying information technology solutions to deliver business value while also complying with regulatory and security requirements.
- ***IT Professionals*** who are responsible for ensuring information technology solutions have adequate cybersecurity while also delivering value to the business or organization.
- ***Business or Organizational Leadership*** who are responsible for achieving business objectives while using information technology systems and protecting sensitive and valuable information.
- ***Business or Organization IT Representative*** who are responsible for delivering business capabilities using information technology and complying with cybersecurity requirements.
- ***Students*** who are learning about business, information technology, or cybersecurity and who need to understand the challenges of delivering effective cybersecurity solutions.

Why Did the Authors Write This Book?

The authors wrote this book based upon personal experiences fighting advanced persistent threats and other modern cyberadversaries. Using the *conventional* cybersecurity architecture of perimeter defenses and endpoint protections was not adequate against the adversaries. The authors realized they needed more resources than were actually available. Not only did they need a new cyberdefense architecture, but they also needed an architecture to coordinate an entire cyberdefense program that allowed them to explain to business leaders what they were doing and why.

The challenge to a cyberdefense program is about much more than buying cybersecurity technologies and deploying them. Without budget, those technologies will never be purchased. Without executive backing, the budget will never materialize. Without clear communications, executive backing will never be obtained. Without good organization, clear communications are impossible.

Figure I-3 delineates how a successful cybersecurity program needs to facilitate the coordination of policy, IT life cycle, cybersecurity assessments, and programmatics. The IT life cycle consists of strategy, engineering, and operation functions. Programmatics include the organization of people, budget, and technology. These major components work together to guide, build, and operate an enterprise cybersecurity program.

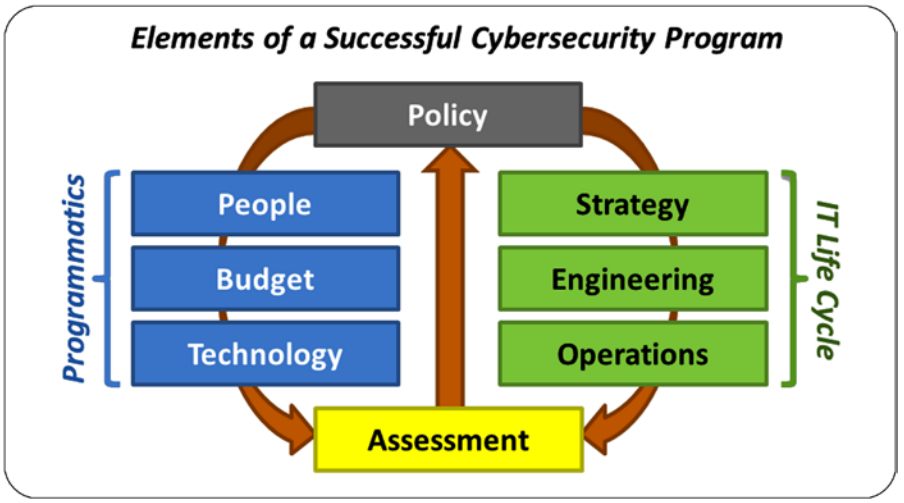

Figure I-3. *A successful cybersecurity program effectively coordinates cybersecurity policy and assessment with the IT life cycle and cybersecurity programmatics.*

A challenge is finding a single framework that can satisfy all these cybersecurity program needs. As the authors looked at major control frameworks and methodologies, they found themselves running into challenges that included the following:

- ***Policy frameworks*** did not align well with how people are typically organized or with how cybersecurity is usually assessed.
- ***Programmatic frameworks*** focus on business considerations and deal with cybersecurity at a high level of abstraction such that their guidance is not actionable, except in the most general of terms.

- ***IT life cycle frameworks*** deal with cybersecurity in broad terms and generally do not consider how cybersecurity needs to be decomposed for management and reporting purposes.
- ***Assessment frameworks*** tend to group cybersecurity controls and capabilities in ways that are not aligned with how people or budgets are typically organized.

An Enterprise Cybersecurity Architecture

As the authors looked at existing frameworks and methodologies, they developed a set of requirements for an effective enterprise cybersecurity architecture that addresses the cybersecurity program needs they encountered. They observed that an effective cybersecurity architecture needs to include the following requirements:

- It needs to tie together policy, programmatics, IT life cycle, and assessments using a single framework for delegation and coordination.
- It needs to break down enterprise cybersecurity into a number of sub-areas to communicate that there is more to effective cybersecurity than just firewalls and anti-virus software.
- Sub-areas need to align relatively well with real-world skills of cybersecurity professionals, budgets supporting those professionals, and technologies purchased and maintained with the budgets.
- Sub-areas need to enable quick and efficient reporting of cybersecurity status so that executives can understand the *big picture* of what is and is not working well.
- Sub-areas need to support the business decision-making process and help leaders define strategy and prioritization.

To satisfy these requirements, the authors envision a new framework that they simply call the *enterprise cybersecurity architecture*. This framework partitions enterprise cybersecurity into 11 functional areas and then focuses on 113 capabilities within those functional areas, rather than specific products, technologies, or processes.

When the authors organize a cybersecurity program in accordance with this architecture, they can show an entire enterprise cybersecurity posture on a single slide. Users of this architecture can express enterprise cybersecurity needs and challenges to their leadership in straightforward and intuitive ways. This information helps enterprise leadership make informed business decisions regarding how to allocate scarce resources to protect the enterprise.

Figure I-4 depicts an early, *simplified* cybersecurity status dashboard that came out of the analysis of various control frameworks. Figure I-4 lists the 11 functional areas of the enterprise cybersecurity architecture and then shows the overall status for each functional area along with a corresponding status of supporting capabilities. The figure shows the enterprise's entire cybersecurity posture on one slide. Showing this high-level, comprehensive status helps enterprise leadership envision areas for improvement. With this larger perspective, business leaders readily understand a single cybersecurity technology is not going to radically change the overall security posture. However, when the cybersecurity capabilities are taken in aggregate, they can make a significant difference.

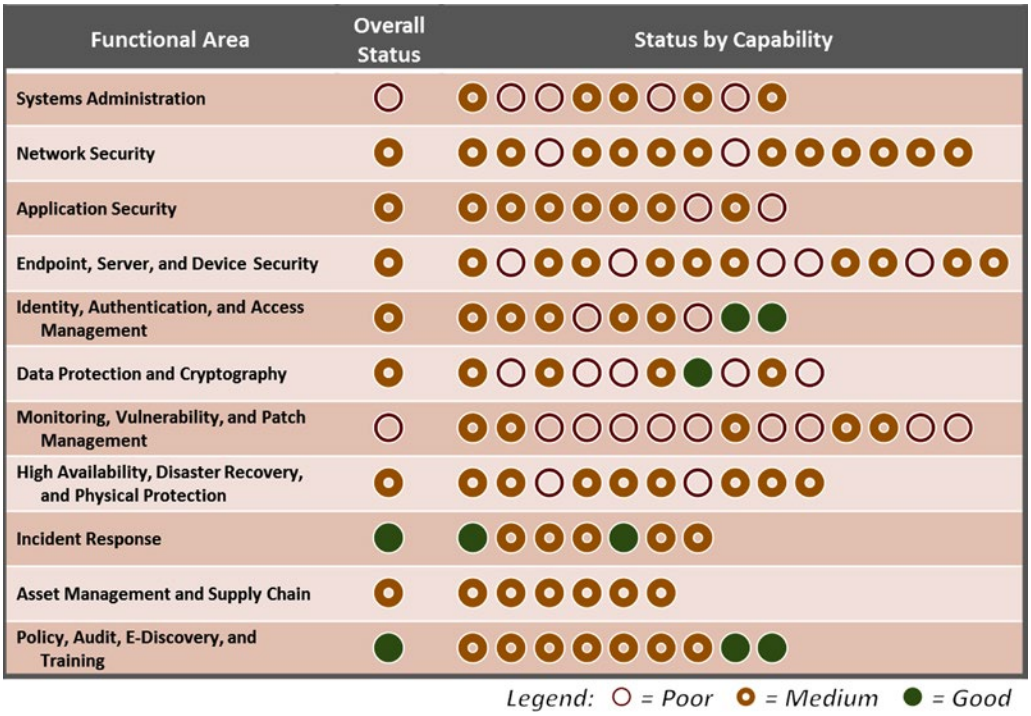

Figure I-4. *An enterprise cybersecurity architecture enables security leadership to manage and report on the status of the enterprise's cybersecurity program in a straightforward and intuitive manner.*

Figure I-4 lists all the functional areas and indicates which ones have the strongest capabilities and which ones have the weakest. Systems Administration and Monitoring, Vulnerability, and Patch Management functional areas are the weakest and most likely need investment for improvement. Incident Response and Policy, Audit, E-Discovery, and Training functional areas are the strongest and probably do not need significant focus for the moment.

For executives, being able to see inside a cybersecurity program without becoming buried in the details is important. For security practitioners, this dashboard provides actionable value as well.

Each dot in the capabilities section represents a security capability in the enterprise, such as protocol filtering, logging, or data analytics. Each one of these capabilities can be tracked and its status reported. Even here, with only three levels of status—perhaps aligning with *weak*, *medium*, and *strong*—practitioners can see which functional areas need the most work and which capabilities within those functional areas should be improved. The enterprise cybersecurity architecture supports all levels of the program.

A Complete Cybersecurity Program

Many frameworks describe the components that go into a cybersecurity architecture; however, few of them speak to the overall cybersecurity program process or cycle. Figure I-5 depicts the high-level cybersecurity program cycle consisting of a number of programmatic steps that occur in a cyclical manner to manage, assess, improve, and operate the enterprise's cybersecurity.

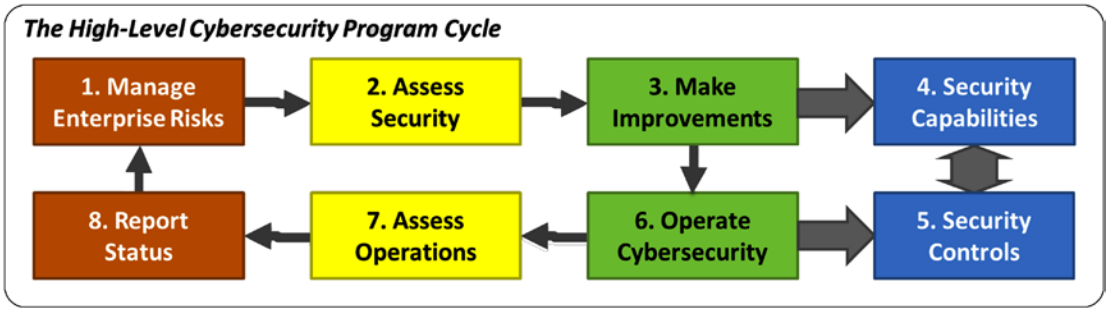

Figure I-5. *A successful enterprise cybersecurity program is an ongoing cycle of risk management, security assessment, improvements against security capabilities and controls, security operations and operational assessment, and finally reporting of status internally and externally.*

Figure I-5 shows this program cycle as a series of steps that are executed in the following cyclical manner:

1. ***Manage Enterprise Risks*** involves assessing risks to the enterprise and scoping enterprise IT systems to contain those risks and deploy mitigating controls and capabilities.
2. ***Assess Security*** involves evaluating the security that is currently deployed to assess its effectiveness and comprehensiveness compared to the negotiated business need.
3. ***Make Improvements*** involves planning improvements to enterprise cybersecurity by deploying or improving technologies and processes.
4. ***Security Capabilities*** are what are delivered by cybersecurity technologies and processes and what enable the enterprise to accomplish its cybersecurity objectives.
5. ***Security Controls*** apply those capabilities to address specific concerns, providing prevention, detection, forensics, or audit of the behavior that is of interest.
6. ***Operate Cybersecurity*** involves operating cybersecurity technologies, processes, capabilities, and controls to deliver cybersecurity to the enterprise.
7. ***Assess Operations*** involves measuring cybersecurity performance to understand what cybersecurity threats are occurring and how well defenses are serving to counter those threats.
8. ***Report Status*** involves reporting cybersecurity status both internally according to internally negotiated frameworks and standards, and externally to regulators, insurers, and other interested parties.

Combining these eight steps provides the major components of a complete cybersecurity program. This program and the cybersecurity architecture that enables it are valid for an organization of 100 people or a corporation or government agency of 100,000. The cybersecurity needs for this range of organizations are similar. The enterprise cybersecurity architecture described in this book can be used to develop an effective cybersecurity program for a wide range of corporate or government organizations.

Organization of the Book

This book contains 15 chapters and 9 appendices. The chapters and appendices are organized into six parts, covering different aspects of an effective enterprise cybersecurity program. The book describes the cybersecurity problem and how to implement a cybersecurity program tailored to an enterprise's needs. The appendices are designed to be companions to the chapters. The appendices explain the concepts introduced in the chapters in detail so an enterprise can design, implement, and run an enduring cybersecurity program.

PART I: The Cybersecurity Challenge

The first part of this book is about the cybersecurity challenge and how cybersecurity has changed over the past ten years. Due to this evolution, the cyberdefense methods that worked well in the past are doomed to fail in the future.

CHAPTER 1: Defining the Cybersecurity Challenge

Chapter 1 defines the cybersecurity challenge facing the modern enterprise and discusses the threats against those defenses and why those threats are succeeding at an alarming and increasing rate.

CHAPTER 2: Meeting the Cybersecurity Challenge

Chapter 2 describes how the cybersecurity challenge can be met and how cybersecurity controls and capabilities can be organized to prevent, detect, document, or audit malicious behavior.

PART II: A New Enterprise Cybersecurity Architecture

Part II introduces a new enterprise cybersecurity architecture that is designed to organize and manage every aspect of an enterprise cybersecurity program, including policy, programmatics, IT life cycle, and assessment.

CHAPTER 3: Enterprise Cybersecurity Architecture

Chapter 3 describes the new enterprise cybersecurity architecture and explores its 11 functional areas in terms of their goals and objectives, threat vectors, and underlying capabilities.

CHAPTER 4: Implementing Enterprise Cybersecurity

Chapter 4 discusses how to implement the new enterprise cybersecurity architecture by identifying security scopes, defining security policies, and selecting security controls to counter anticipated threats.

CHAPTER 5: Operating Enterprise Cybersecurity

Chapter 5 explains how to operate enterprise cybersecurity capabilities and processes, introducing the 17 operational processes and 14 supporting information systems essential to effective enterprise cybersecurity.

CHAPTER 6: Enterprise Cybersecurity and the Cloud

Chapter 6 discusses how cloud computing is different from the conventional data center and explains how the new architecture needs to be tailored to be used for cloud computing environments.

CHAPTER 7: Enterprise Cybersecurity for Mobile and BYOD

Chapter 7 describes the trends of mobile computing and Bring Your Own Device (BYOD), and how these two trends solve problems and introduce challenges for the new architecture.

PART III: The Art of Cyberdefense

Part III discusses the art of the cyberdefense, and how the new architecture is deployed and used to provide effective risk mitigation and incident response for cybersecurity crises.

CHAPTER 8: Building an Effective Defense

Chapter 8 examines why attackers have great success against legacy cyberdefenses, the steps of the attack sequence and how to disrupt them, and how to layer cyberdefenses so they effectively thwart targeted attacks.

CHAPTER 9: Responding to Incidents

Chapter 9 describes the incident response process in detail by considering what the enterprise needs to do on an ongoing basis to investigate, contain, and remediate cybersecurity incidents when they occur.

CHAPTER 10: Managing a Cybersecurity Crisis

Chapter 10 discusses how severe cybersecurity incidents become crises and how the enterprise must behave differently in a crisis situation while it struggles to restore normal operations.

PART IV: Enterprise Cyberdefense Assessment

Part IV establishes a methodology for quantitatively and objectively assessing cybersecurity using the enterprise cybersecurity architecture and then mapping those assessments against major frameworks for reporting purposes.

CHAPTER 11: Assessing Enterprise Cybersecurity

Chapter 11 explains the cybersecurity assessment and auditing process, and provides four worked-out examples using the new architecture to assess cybersecurity posture and effectiveness.

CHAPTER 12: Measuring a Cybersecurity Program

Chapter 12 provides a comprehensive method for objectively measuring an enterprise's cybersecurity by looking at risk mitigations, cybersecurity functional areas, and security operations.

CHAPTER 13: Mapping Against Cybersecurity Frameworks

Chapter 13 explains how to take the results of an enterprise cybersecurity assessment and map them against other cybersecurity frameworks for the purpose of evaluation, audit, or compliance reporting.

PART V: Enterprise Cybersecurity Program

Part V brings together the concepts of the rest of the book into a comprehensive enterprise cybersecurity program that combines assessment, planning, prioritization, implementation, and operations.

CHAPTER 14: Managing an Enterprise Cybersecurity Program

Chapter 14 explains the cybersecurity program management process and shows how the enterprise can use it to manage cybersecurity decision-making and prioritize improvements to get the best possible value for the investment.

CHAPTER 15: Looking to the Future

Chapter 15 concludes the book by discussing the evolution of generations of cyberattacks and cyberdefenses, and how enterprise cybersecurity architecture will evolve over time to support the enterprise's needs now and in the future.

PART VI: Appendices

The appendices provide greater detail than the chapters and provide important details and examples for cybersecurity practitioners who want to use the enterprise cybersecurity architecture described in this book.

APPENDIX A: Common Cyberattacks

Appendix A describes many of the cyberattacks that are common today, explaining their impact, methods and consequences, and potential defenses used to counter them.

APPENDIX B: Cybersecurity Frameworks

Appendix B describes a number of the major cybersecurity frameworks that are in common use at the time of publication, explaining some of the philosophy behind each framework and how each one *slices and dices* cybersecurity into components.

APPENDIX C: Enterprise Cybersecurity Capabilities

Appendix C details the 113 cybersecurity capabilities of the new architecture, organized into its 11 functional areas.

APPENDIX D: Sample Cybersecurity Policy

Appendix D provides a sample enterprise information security policy document, organized into the 11 functional areas of the new architecture described in this book.

APPENDIX E: Cybersecurity Operational Processes

Appendix E contains detailed flowcharts for the 17 operational processes of enterprise cybersecurity, and it also introduces the 14 supporting information systems.

APPENDIX F: Object Measurement

Appendix F introduces the Object Measurement methodology for objective assessment, and explains how to use it to measure and report enterprise cybersecurity architecture effectiveness.

APPENDIX G: Cybersecurity Capability Value Scales

Appendix G contains detailed, example Object Measurement value scales for measuring the performance of each of the 113 enterprise cybersecurity architecture capabilities, grouped by the 11 functional areas.

APPENDIX H: Cybersecurity Sample Assessment

Appendix H provides an example enterprise cybersecurity assessment using the methodology contained in this book, providing multiple levels of detail showing how different types of assessment can be performed.

APPENDIX I: Network Segmentation

Appendix I describes a simple methodology for network segmentation that is suitable for countering many advanced threats and provides a good balance between *containment and security* versus *complexity and cost*.

Glossary

The Glossary provides an explanation of the cybersecurity terms used in this book, expressed in *plain English* for the non-technical reader.

Bibliography

The Bibliography provides additional literature for readers who wish to explore extensions to material addressed in this book and who wish to explore alternatives to what this book addresses.

Index

The Index provides a means for the reader to locate concepts and other material the book addresses in a timely manner.

PART I

The Cybersecurity Challenge

CHAPTER 1

Defining the Cybersecurity Challenge

It appears that lately cybersecurity is in trouble, or at least going through a difficult time. If you are reading this book, you are one of the people trying to make cybersecurity work despite daunting challenges and information technology (IT) environments seemingly ill-suited to facing those challenges. The authors share your concerns.

This book is about building *effective cybersecurity* that works against advanced cyberthreats, despite the challenges. Effective cybersecurity works when you are faced with an adversary who is well-funded, intelligent, sophisticated, and who does not give up at the first sign of cyberdefense. Effective cybersecurity evolves over time to handle increasingly sophisticated adversaries in an increasingly interconnected world. Effective cybersecurity involves cybersecurity as a partner, coach, and scorekeeper for IT, rather than just a naysayer standing in the way of progress.

This book describes a comprehensive framework for managing an enterprise cybersecurity program that is pragmatic, realistic, and suited to battling today's cyberthreats. This book's field-proven framework has been used to run large-scale cybersecurity efforts against advanced nation-state adversaries and talented individual hackers. This flexible framework is designed to manage cyberdefenses against today's sophisticated cyberthreats, as well as tomorrow's next-generation cyberthreats.

The Cyberattacks of Today

Compared to today, cybersecurity used to be relatively simple. The major cyberthreats were viruses, worms, and Trojan horse. These cyberthreats randomly attacked computers directly connected to the Internet, but posed little enterprise threat. Inside enterprise networks with firewalls on the outside and anti-virus protection on the inside, the enterprise appeared to be protected and relatively safe. Occasionally an incident would occur and cyberdefenders would rally to fight it, but once the defenders understood the malicious code, detecting it and defeating it was straightforward.

Then, slowly but surely, a transformation started to take place. Cyberattackers started getting inside enterprise networks, and once they were inside they operated surreptitiously. Cyberattackers took control of infected machines and connected them to remote command-and-control systems. They captured usernames and passwords, and then used them to connect to systems for stealing data or money. Cyberattackers exploited vulnerabilities inside the enterprise to move laterally among computers on the network and capture the credentials of more and more people within the enterprise. Finally, cyberattackers escalated privileges and got control of the systems administrator accounts in charge of everything. Once these attackers got administrative control of the enterprise, they were able to do anything they wanted.

"We are using outdated, conventional defenses to guard against cutting-edge, innovative malware. We are no more prepared to do this than a 19th century army trying to defend itself against today's electronic weaponry." —FireEye.[1]

In recent years, this trend has played out in more and more spectacular breaches hitting the headlines. Just a couple of the severe intrusions include the following:

- In 2011, RSA's enterprise was breached and the security keys for many of its customers were believed to have been stolen. This breach prompted RSA to replace millions of its SecureID tokens to restore security for its customers. This breach is disconcerting because RSA is one of the oldest and most established cybersecurity brands.
- In 2013, Target's point of sale (POS) network was compromised, resulting in the loss of personal information and credit card numbers for over 40 million customers. The costs of this breach, particularly when reputational damage and lawsuits are taken into account, will likely be huge.
- In 2014, Sony Pictures Entertainment reported attackers had infiltrated its environment and disabled almost every computer and server in the company. This cyberattack brought the company to its knees and resulted in the public release of thousands of proprietary documents and e-mail messages.
- In 2014, a German steel mill was affected by a hacking incident that caused one of its blast furnaces to malfunction. This resulted in significant physical damage to the plant and its facilities.
- In 2015, Anthem reported its IT systems had been breached and personal information on over 80 million current and former members of their healthcare network was compromised, which included the US government's Blue Cross Blue Shield program.

These intrusions are but a handful of the myriad of cybersecurity breaches that have occurred recently. However, these breaches are indicative of some of the major trends. Cyberattackers are now targeting personal identities, financial accounts, and healthcare information and getting such information on millions or tens of millions of people in a single breach. Cyberattackers are taking control of industrial equipment and causing physical damage to plants and equipment. Thankfully, no one has been hurt so far, but given the current trends it may just be a matter of time.

These headlines seem to indicate that the attackers have gotten the upper hand, at least for now. The question is, "What has changed and how can the defenders recover?"

The Sony Pictures Entertainment Breach of 2014

In November 2014, Sony Pictures Entertainment employees got to the office to find themselves in the crosshairs of an IT horror story. Their computers had been taken over. Instead of displaying logon prompts, office productivity, and corporate web sites, they were completely nonfunctional and displayed a message from an organization claiming to be the Guardians of Peace. By the end of the day, most of the computers at Sony Pictures had been completely disabled, sharply impairing the company's business while they

[1]FireEye, "Advanced Malware Exposed," www2.fireeye.com/wp_advmalware_exposed.html, 2011.

recovered data and IT systems. The cyberattackers then went on to publish proprietary data from Sony Pictures, including salaries and personal e-mails of its senior executives. The breach caused a media sensation due to the salaciousness of the data published. The breach also caused earthquakes in the cybersecurity industry, as the IT community got a glimpse of what a devastating cyberattack could do.

Key lessons learned include the following:

- The Sony hack is significant, not because the attackers did something no one could do before, but because the attackers did what cyberattackers have been able to do all along, but have chosen not to. The security industry has been warning for years that cyberattackers could bring a company to their knees. The Sony hack put the reality of this possibility in full view of the press and the public.
- It is reasonable to expect that Sony's cyberdefenses were consistent with industry norms and reflected what is and is not being done at a myriad of other companies around the world. In fact, Sony Pictures was likely better defended than most enterprises due to its size and prominence. One has to ask, "Is this an indication of how vulnerable everyone is to a devastating cyberattack?"
- The effectiveness of the Sony hack was likely amplified by the consolidation of IT systems administration that has occurred over the past 20 years. In the past, a single systems administrator might manage a handful of servers providing, at most, one or two enterprise services. Today, the same administrator may have privileged access to a hundred systems, or even thousands. If attackers can get control of that one person's administrative credentials, the damage they can do is devastating.
- These types of attacks show how professional attackers, who understand how modern IT works and how it is managed, can effectively turn an enterprise's IT infrastructure against it. These infrastructures are largely designed for functionality, not security, and often lack compartmentalization to contain a breach and limit its damage.
- Finally, attacks like Sony's underscore the fear factor that devastating cyberattacks can have on an industry and the nation. What would be the political impact if an individual, an organization, or a nation-state could pull off a hundred Sony-style attacks, all simultaneously?

There is a mega-trend going on here. These types of cyberattacks are moving *down market* over time. In other words, the techniques nation-states were using a couple of years ago are being used by cybercriminals today. The techniques cybercriminals were using a couple of years ago are in commodity malware and viruses today. It is reasonable to expect what was done to Sony Pictures Entertainment will become more common in the future as cyberattack tools and techniques proliferate and become available to larger and larger communities. So, while these types of threats may only be of concern to a small group of top-tier players today, as these threats move down market, they will become more widespread.

The tools and techniques to fight these types of attackers exist today, but they are not cheap or easy to deploy. Also, fighting these cyberattackers requires re-thinking many aspects of IT so that security is *baked in* rather than *bolted on*. One cannot simply buy a widget and be immune to Sony-style attacks. Just as banks have to invest in alarms and security guards, enterprises have to invest in people doing the dirty, grunt work of cybersecurity, day in and day out. Enterprises have to be constantly evolving their defenses. Cybersecurity defense is an arms race and the attackers are smart, competent, and ill-intended. The attackers who hit Sony Pictures Entertainment are advanced, persistent, and very, very threatening.

Advanced Persistent Threats

In fact, these major breaches point to the rise of a new type of adversary, the advanced persistent threat (APT). These attacks are of great interest, not because they are mysterious or particularly advanced, but because they mark the widespread professionalization of cyberattacks. An APT attacker is skilled in the art of cyberattack and leverages IT technologies effectively to breach enterprises and systematically bypass all of their protections, one at a time. What makes APT different from earlier cyberattack types is the persistence of the attack. Back in the days of viruses and Trojan horses, cyberattacks were generally regarded as somewhat arbitrary. A software developer created a piece of malware and sent it out onto the Internet to propagate and spread. Either it propagated or it did not. Where it propagated was generally arbitrary, determined more by luck than by any specific direction from the developer.

APT makes cyberattacks much more focused and effective because now they are under the control of an intelligent actor who has an objective to achieve. If the attackers' goal is to break into a bank or a merchant, they persist in their attack and try multiple angles and approaches until they are successful. If their goal is to break into a company and steal corporate secrets, they persist in pursuing that goal until they succeed. If their goal is to break into a government and steal national security information, they persist in trying to find weaknesses in the government's networks and computers until they find them and exploit them.

In a conventional attack, defenses only need to block the malware, and it will move on to other targets. Simply having defenses is no longer effective when a single mistake can be exploited by an opportunistic attacker. An APT attacker constantly adjusts the attack to get past the latest round of defenses. *Given enough time, an APT attacker eventually gets through*. To stop the attacker from getting through the defenses, the defenses have to work perfectly and be maintained perfectly. Any mistake on the part of the defenders is promptly exploited by the attacker, who is waiting for mistakes to occur. APT requires a new type of defense method—one that adapts to the attack as quickly as the attack adapts to the defense.

Waves of Malware

Looking at the adversaries' techniques, tools, and technologies and corresponding cyberdefenses over the past 20 years, one can see there have been a number of generations, or *waves,* of malware technologies infecting computers and propagating on networks. These can be grouped into different categories based upon their characteristics and behaviors, including the following:

1. ***Static Viruses*:** The first malware wave is static viruses that propagated from computer to computer via floppy disks and boot sectors of hard drives. These viruses propagated themselves, but few of them actually impacted system operations.

2. ***Network-Based Viruses*:** The second malware wave is network-based viruses that propagated across the open Internet from computer to computer, exploiting weaknesses in operating systems. Computers were often directly connected to each other without firewalls or other protections in between.

3. ***Trojan Horse*:** The third malware wave is Trojan malware that propagates across the Internet via e-mail and from compromised or malicious web sites. This malware can infect large numbers of victims, but does so relatively arbitrarily since it is undirected.

4. ***Command and Control*:** The fourth malware wave includes command and control features that allows the attacker to remotely control its operation within the target enterprise. Compromised machines then become a foothold inside of the enterprise that can be manipulated by the attacker.

5. ***Customized*:** The fifth malware wave is custom malware developed for a particular target. Custom malware is sent directly to specific targets via phishing e-mails, drive-by websites, or downloadable applications such as mobile apps. Because the malware is customized for each victim, it is not recognized by signature-based defenses.

6. ***Polymorphic*:** The sixth malware wave is polymorphic malware designed not only to take administrative control of victim networks, but also to dynamically modify itself so it can continuously evade detection and stay ahead of attempts to remediate it.

7. ***Intelligent*:** The seventh malware wave is malware with intelligence to analyze a victim network, move laterally within it, escalate privileges to take administrative control, and extract, modify, or destroy its target data or information systems. Intelligent malware does all of these actions autonomously, without requiring human intervention or external command and control.

8. ***Fully Automated, Polymorphic*:** The eighth malware wave is fully automated, polymorphic malware that combines the features of the sixth and seventh waves. This malware takes control autonomously and dynamically evades detection and remediation to stay one step ahead of defenders at all times.

9. ***Firmware and Supply Chain*:** The ninth malware wave takes the eighth wave to its logical conclusion by delivering malware capabilities through the supply chain, either embedded in product firmware or within software products before they are shipped. Such malware is embedded in products when they are built, or at such a low level in the product firmware that they are virtually undetectable. By delivering malware in this manner, it is difficult for cyberdefenders to differentiate the supply chain malware from the other features *coming from the factory*.

Many people are familiar with the first three waves of cyberattacks, which represent the majority of consumer-grade cyberthreats and many of the attacks covered in the popular press. Enterprises are experiencing malware waves four, five, and six on a regular and increasing basis. However, these waves of malware are little-understood outside of specialized cybersecurity fields. Nation-state cyberattackers use malware waves seven, eight, and nine. Such waves require considerable resources and expertise. These waves are sophisticated malware packages designed to penetrate the most developed cyberdefenses.

All of these malware technologies are proliferating over time. Not too long ago, waves four, five, and six were solely in the domain of the nation-state attacker. Today these are in the hands of cybercriminals; the malware waves are moving *down market*. It is reasonable to expect in the future that such sophisticated tools will be in the hands of the casual attacker as well. The cyberattackers are not sitting still, and their tools are constantly evolving.

Types of Cyberattackers

Who are these mysterious cyberattackers hacking into systems and causing these headlines? Obviously, they are people, somewhere in the world, who choose to create, distribute, and use malware or other tools or techniques to do things on computers they shouldn't be doing. As depicted in Figure 1-1, these people can be grouped into five categories based on their intent and objectives.

Figure 1-1. *Cyberattacker categories can be distinguished by their intent and objectives distinguishable by their intent and objectives.*

There can be significant overlap in the tools and technologies used by these groups. These five cyberattacker categories are described in the following sections.

Commodity Threats

Commodity threats are the random malware, viruses, Trojans, worms, botnets, ransomware, and other threats that are out propagating on the Internet all the time. Strictly by chance, commodity threats are undirected and may end up inside of the enterprise at any time. Commodity threats may exploit vulnerabilities or other cyberdefense weaknesses, but they do not adjust or adapt to work their way around protections that are in place.

Commodity threats can be destructive, although the amount of damage they can do is usually pretty limited. However, they can also be the starting point for more dangerous, targeted threats. Targeted cyberattackers may start their efforts by going to botnet operators and purchasing access to computers and servers that are already compromised inside the target environment. This purchased access can make the attackers' initial entry into the enterprise easier and save them valuable time and money.

For the purposes of this book, commodity threats are undirected and opportunistic. Defenders only need to block the threat's attack vector, and the defenders are safe. For the other cyberattack threat categories, simply blocking the initial attack vector is only a start.

Hacktivists

Activist hacking, or hacktivism, consists of targeted attacks. Hacktivists use hacking to make a public or political statement. Their goal is to use hacking to bolster their cause or embarrass their adversaries. Hacktivism may be used against individuals, enterprises, or governments, depending on the situation and the particular objectives of the hacktivists.

Hacktivists, because of their activist ideology, 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. Hacktivists conduct their attacks with an explicit objective of getting it covered by the press, their message communicated, and their adversaries embarrassed.

Since hacktivists are frequently individuals acting alone or small organizations with only limited resources, hacktivists tend to use mostly commodity tools and techniques that are widely available on the Internet. The defenses to protect against these tools and techniques are also usually widely available. The hacktivists operate by taking advantage of vulnerabilities that are unpatched or otherwise open to exploitation. Hacktivists will try and try again until the defenders make a mistake that allows them to accomplish their goal.

Organized Crime

Like hacktivism, organized crime attacks are targeted. Criminals and criminal organizations have found there is serious money to be made on the Internet. There are a number of factors that make the Internet particularly attractive to criminal elements:

- ***Easy Access*:** On a global, interconnected network the so-called good neighborhoods and bad neighborhoods are just a click apart. Criminals can touch anyone in the world, without leaving their easy chair.
- ***Lack of Attribution*:** On the Internet, it can be notoriously difficult to track down attackers, especially when they take measures to cover their tracks. When the victims are in one country and the criminals in another country, it only gets harder to track down the attackers.
- ***Wholesale Data*:** Why steal money from one person at a time when, with only a little more effort, you can rob the bank instead? Criminals have found that with the consolidation of data into huge corporate databases, wholesale data theft can be shockingly easy to carry out.

These factors have turned data theft into big business. Big money can be made by those who get away with the big heists. When stolen credit cards or social security numbers go for $1 each on the black market and medical records go for $10 or more, the attacker who can steal a million records can make real money. This money, in turn, goes to support an entire shadow industry of players, suppliers, and supporting actors who are ready to help out and lend their services in exchange for a cut in the loot.

When considering cybercriminals, it is important to remember there are many ways to make money through cyberattacks. Many of those methods have nothing to do with stealing credit card numbers. Cyberattackers can get control of business banking accounts and use online banking to drain corporate accounts by wiring money to themselves. Cyberattackers can encrypt corporate data using ransomware malware and then blackmail the business to get its data back. Cyberattackers can compromise employee accounts and re-route payroll direct deposit to their own accounts. There is no limit to how creative cybercriminals get in monetizing the fact that they can compromise people, accounts, and computers at their victims' enterprises.

Espionage

What organized crime starts, espionage agents take to the next level. Cybercriminals are relatively easy to understand since their objectives are straightforward. Cybercriminals seek to gain access to computers, accounts, and networks and then exploit the access to either directly steal money or steal data that can then be quickly and easily turned into money. Cyberespionage, on the other hand, is a little more complex in its objectives and how it carries them out. Certainly, there is a financial driver, but other drivers are much less straightforward.

Cyberespionage centers on stealing trade secrets for commercial advantage or national secrets for political or military advantage. In the cases of international business, these two interests can be closely aligned, and multinationals can find themselves being targeted by national intelligence agencies working in close collaboration with their international competition. Whereas in the United States, business and government have an arms-length relationship, in many countries such a relationship is not always the case.

The secrets stolen may be surprising. All enterprises have the "crown jewels" of blueprints, formulas, or software code that are considered critical to success. However, there is plenty of other information such as organizational charts, budgets, project schedules, and even meeting minutes that are vitally useful to the competition. All of this information may be subject to espionage efforts on the part of adversaries, particularly multinational ones.

Cyberespionage practitioners frequently use APT-style methods, not because such methods are the only way to get the job done, but because they tend to be very effective against enterprises with legacy-style cyberdefenses. Why bother hacking the CEO's laptop when, for the same amount of effort, you can get control of every laptop in the enterprise? Once agents get administrative control, they can then steal proprietary data at will.

Cyberespionage campaigns can be conducted at the nation-state level, and these campaigns can be made up of multiple parts. Unfortunately for some enterprises, their cyberespionage experience may simply be because they are a stepping stone in a campaign focused on getting to other, unrelated objectives. For example, espionage agents may hack a hospital simply to get identity information on one of its patients who is of interest to them. A popular web site may be hacked simply because it is frequented by people at enterprises that the espionage agents are targeting. Cyberespionage is a serious issue, and the campaigns can involve complex webs of target individuals and enterprises as the agents work their way from their starting points toward their objectives.

Cyberwar

Whereas espionage is generally focused on stealing information, cyberwar is about damaging the ability of enterprises 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. The possibility of cyberintrusions causing physical harm, injuries, or death is a disconcerting one. Everything is increasingly computerized and networked—the damage that can be done from cyberspace continues to increase.

Cyberwar has a cousin, cyberterrorism, which is conducted using the same techniques but by unaffiliated individuals or terrorist organizations. While cyberwar is waged to support national interests, cyberterrorism is done for an activist agenda, or it may simply be performed for the sake of anarchy and destruction for its own sake. The effects, particularly the psychological effects, are the same either way. Both of these activities are done using similar tools and techniques, employing denial of service, data destruction, or control system manipulation to accomplish their goals.

There have been several instances of cyberwar in recent years. In 2007, Estonia's Internet infrastructure was targeted by a series of cyberattacks that interfered with telephone, financial, and government operations. The notorious Stuxnet worm infiltrated the Iranian nuclear program and ruined nuclear centrifuges required for enriching uranium. The 2012 cyberattack on Saudi Aramco resulted in tens of thousands of computers having to be replaced or rebuilt. Many nations have cyberwarfare capabilities, and it is an increasing factor even in conventional conflicts.

The Types of Cyberattacks

Regardless of the objective or techniques, there are generally three things that cyberattacks can do to an enterprise or its data, as shown in Figure 1-2. Cyberattacks compromise confidentiality by stealing data, compromise integrity by modifying data, or compromise availability by denying access to data, services, or systems. Some attacks may combine two or more of these types in a single attack, but these three cyberattack types are the building blocks for most malicious cyberactivities. Appendix A provides descriptions of common cyberattacks that have one or more of these effects on their victim enterprises. Cyberdefenses must focus on protecting the confidentiality, integrity, and availability of data and the IT systems that process it.

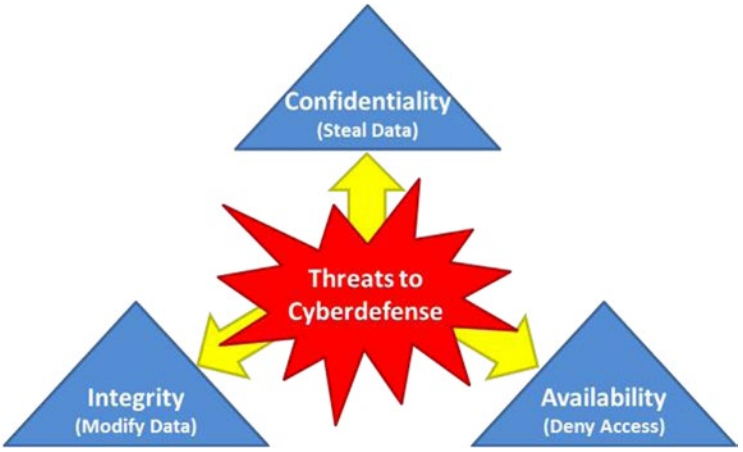

Figure 1-2. *The damage caused by threats to cyberdefense can be characterized by losses of confidentiality, integrity, or availability.*

Confidentiality: Steal Data

Confidentiality breaches are the ones most often making the headlines today. Social security numbers, credit card numbers, bank account information, electronic health records, and confidential corporate secrets and executive correspondence are just some examples of the data being stolen from enterprises and sold to the highest bidder. Attacks intended to steal data often focus on stealth, at least at first, to penetrate the target enterprise, get to the target data, and exfiltrate it without being noticed. On the other hand, once the victim enterprise is aware that a breach is in progress, the attackers may become significantly bolder, especially to finish an attack that is already ongoing.

Confidentiality breaches focus on getting access to the data where it resides, which can be any of a number of at-rest and in-transit locations:

- ***Databases*:** The most obvious place to find large pools of data is in the databases where it resides. However, these systems tend to be relatively well protected deep inside the enterprise architecture.
- ***Backups*:** Enterprise databases containing critical business and customer data should be backed up. Interestingly, these backups frequently end up being in a myriad of locations where data is replicated to disk, to tape, to non-production test systems, and to virtual machine snapshots, all on a regular basis. These secondary backup locations frequently do not get much security consideration and may be vulnerable to attack, particularly if they store their data unencrypted.
- ***Application Servers*:** Even the well-protected databases have to make their data available somehow, and the front-end application servers with access to that data are frequently directly connected to the Internet. Breaches of these systems can be used to get access to data through the applications, bypassing encryption and other protection methods.
- ***Systems Administrators*:** The Achilles' heel of most enterprises is the systems administrators and the credentials they use to administer systems. If attackers can get access to these credentials, they can bypass all other data protections and frequently do so with little or no audit trail to reveal their actions.

Integrity: Modify Data (Steal Money)

Integrity breaches are getting far less attention than confidentiality breaches these days. It is realistic to expect the prominence of integrity breaches will increase as attacks continue to gain in sophistication. Integrity attacks involve modifying data, which can result in various impacts to include the following:

- Reputational impacts if that data is public-facing information such as web sites
- Financial reporting impacts if it is financial data, particularly for a publicly traded corporation
- Losses of actual money if the data that is changed is bank routing numbers or financial commands to banks handling corporate accounts

Some integrity attacks of particular interest include the following:

- ***Hijacking*:** Altering infrastructure data about Internet properties such as domain names, social media identities, or registered network locations. Much of the Internet's *real estate* is purely electronic in nature and secured by nothing more than an e-mail address. Some of these properties can be worth thousands or even millions of dollars.
- ***Sarbanes-Oxley*:** In the wake of the Enron disaster, the Sarbanes-Oxley regulations were developed to protect the integrity of financial data published by publicly traded corporations. Unauthorized changes to financial data can have serious audit and regulatory consequences for the affected corporation.
- ***Online Banking*:** With the rise of online banking, enterprises have online access to business banking accounts that can include payroll, investments, stock funds, and other assets worth thousands or millions of dollars. Attackers who can get access to the credentials controlling these accounts can quickly steal large amounts of money. Moving the money through multiple intermediaries in multiple countries makes it impossible to trace or prosecute the attackers.
- ***Direct Deposit*:** Similarly, with payroll services Internet-enabled and providing online access to pay stub information and bank direct deposit settings, employees are vulnerable to thefts where their paychecks are re-routed to an attacker's accounts. If a single attacker can redirect paychecks of a number of highly compensated individuals all at the same time, it is possible to get away with a large sum of money quickly.
- ***Vandalism*:** Malicious actors deface web sites or other public materials with the intent of embarrassing the victim. Internet-facing systems can be hard to protect perfectly. A single vulnerability or configuration mistake can be all it takes to allow an attacker to strike.

Availability: Deny Access

The third type of cyberattack is to affect the availability of systems and deny access to them. Attacks causing denial of service can be difficult to diagnose, especially if systems are impaired but not disabled. Often the systems are impaired when the attack causes failures by overwhelming systems and infrastructure. In general, deliberate availability attacks can be grouped into three categories:

- ***Distributed Denial of Service (DDoS)*** attacks are used to effectively disable services in the victim enterprise or country. These techniques have been used in the past several years, and they can take significant portions of the victim's Internet capabilities offline for some time until they are mitigated.
- ***Targeted Denial of Service*** attacks involve hacking into the victim and then disabling systems so that they have to be rebuilt or recovered. Depending on the severity of the damage done, it can take some time for IT personnel to recover systems and restore service, particularly if backups are affected as well as the primary systems.
- ***Physical Destruction*** attacks involve using cyberattacks to cause physical destruction. Stuxnet is the most famous incidence of this type of attack, where a cyberattack sabotaged centrifuges used by the Iranian nuclear program. As more and more critical systems are computer-controlled, these types of attacks will become potentially more dangerous and destructive over time.

The Steps of a Cyberintrusion

How do these cyberattacks occur? For cyberintrusions, where hackers actually take control of computers and accounts inside of the victim enterprise, it is helpful to work out the steps required for the intrusion to succeed. If an enterprise can understand how cyberintrusions occur, then it can design defenses that disrupt, detect, delay, and defeat the attacks after they start, but before they can succeed. Each step in the attack is also an opportunity for defense. The following material delineates steps required for these cyberintrusions to be successful.

Attack Trees and Attack Graphs

In 1999, Bruce Schneier published an article in *Dr. Dobb's Journal* that introduced a methodology for analyzing attacks, called "Attack Trees." An attack tree begins with the objective of the cyberattack (for example, stealing enterprise data) and then works backward to consider the various ways that goal could be accomplished and the steps involved accomplishing the goal. Figure 1-3 depicts a notional attack tree that Mr. Schneier analyzed for the case of trying to break into a safe.

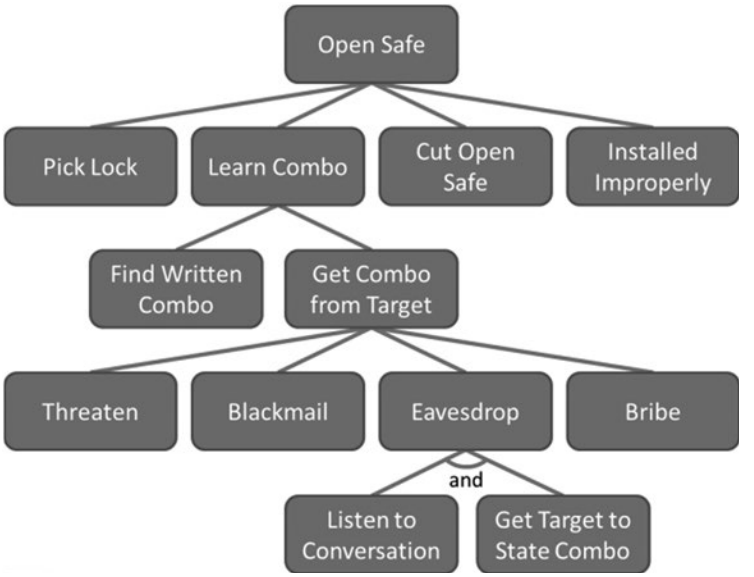

Figure 1-3. *Bruce Schneier introduced attack trees to help analyze the sequence of events involved in a successful attack, starting from the outcome and working backward.*[2]

"Attack trees provide a formal methodology for analyzing the security of systems and subsystems. They provide a way to think about security, to capture and reuse expertise about security, and to respond to changes in security."[3]

What makes this technique interesting from a defensive perspective is that each step in the tree is an opportunity to apply defenses and make the overall attack harder. Those defenses can make the individual step more difficult, expensive, or improbable. The defenses can increase the likelihood the attack step will trigger an alarm and cause the entire attack to be detected. Defenses can also add steps the attack must take before it can succeed. Just as putting the money in a safe means that the attackers then have to figure out how to get into the safe before they can get to the money, putting data into *virtual safes* can have the same effect. It does not make stealing the data impossible as no defense is perfect, but it can make the attack significantly more difficult, time-consuming, and expensive, and it can shift the odds in favor of the defense.

Significant academic research is ongoing using attack trees and a generalized version of attack trees called *attack graphs*. A graph is just like a tree, except that the dependencies can loop back on themselves. Attack graphs have been computed for massive networks. This research shows how vulnerabilities interconnect and how attackers can step from one compromised computer to another until they reach their target. While academically interesting, in practice, this research has shown itself to be of only limited use. Attack graphs of more than a handful of machines that consider more than a handful of potential vulnerabilities quickly become incredibly complex, and defenders have a very difficult time turning the data from these graphs into actionable intelligence that is helpful in designing cyberdefenses.

---

[2]Bruce Schneier, "Attack Trees," *Dr. Dobb's Journal*, December 1999.
[3]Bruce Schneier, "Attack Trees," *Dr. Dobb's Journal*, December 1999.

What kind of attack graph is useful? By using attack tree and attack graph methodologies, it is possible to come up with a generalized model of the cyberintrusion sequence of activities. Cyberdefenders can analyze multiple ways the attackers could accomplish an activity. Defenders can then focus their defenses on disrupting the activity across all potentially vulnerable computers, accounts, and networks. Consequently, the attack tree can be generalized into a model that is simpler to analyze, but almost as powerful in terms of providing specific, actionable results.

When simplified as described, the attack tree gets reduced down to a sequence. This sequence has been given many labels, including *Kill Chain* and *Attack Life Cycle*. For the purposes of this book, this sequence is called the *Attack Sequence*.

Lockheed Martin Kill Chain

In 2011, several researchers from Lockheed Martin published a paper, titled *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*.[4] This paper analyzed Advanced Persistent Threat (APT) attack campaigns and found there was a sequence of seven steps followed by all attackers, and defenses could be applied at each step of the process to attempt to thwart the attack. Figure 1-4 depicts the steps of this process.

Figure 1-4. *Lockheed Martin Kill Chain describes seven steps from reconnaissance through actions on the objective and recommends defenses be designed to align with each of the seven steps in the process.*

Here are the definitions of each of these phases, as described in the original Lockheed paper:

1. ***Reconnaissance*:** Research, identification, and selection of targets, often represented as crawling Internet web sites such as conference proceedings and mailing lists for e-mail addresses, social relationships, or information on specific technologies.
2. ***Weaponization*:** Coupling a remote access Trojan with an exploit into a deliverable payload, typically by means of an automated tool (weaponizer). Increasingly, client application data files such as Adobe Portable Document Format (PDF) or Microsoft Office documents serve as the weaponized deliverable.
3. ***Delivery*:** Transmission of the weapon to the targeted environment. The three most prevalent delivery vectors for weaponized payloads by APT actors, as observed by the Lockheed Martin Computer Incident Response Team (LM-CIRT) for the years 2004–2010, are e-mail attachments, web sites, and USB removable media.
4. ***Exploitation*:** After the weapon is delivered to victim host, exploitation triggers intruders' code. Most often, exploitation targets an application or operating system vulnerability, but it could also more simply exploit the users themselves or leverage an operating system feature that auto-executes code.

[4]Eric M. Hugchins, Michael J. Cloppert, and Rohan M. Amin, Ph.D., "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf, 2011.