INFORMATION SECURITY

PRINCIPLES AND PRACTICES

SECOND EDITION

MARK S. MERKOW • JIM BREITHAUPT

Information Security: Principles and Practices

Second Edition

Mark S. Merkow
Jim Breithaupt

PEARSON

800 East 96th Street, Indianapolis, Indiana 46240 USA

Information Security: Principles and Practices, Second Edition

ISBN-13: 978-0-7897-5325-0
ISBN-10: 0-7897-5325-1

Library of Congress Control Number: 2014937271

Printed in the United States of America

First Printing: June 2014

Associate Publisher
Dave Dusthimer

Acquisitions Editor
Betsy Brown

Development Editor
Jeff Riley

Managing Editor
Sandra Schroeder

Senior Project Editor
Tonya Simpson

Copy Editor
Krista Hansing Editorial Services, Inc.

Indexer
Publishing Works

Proofreader
Paula Lowell

Technical Editors
Tatyana Zidarov
Chris Crayton

Publishing Coordinator
Vanessa Evans

Cover Designer
Alan Clements

Compositor
Trina Wurst

Contents at a Glance

Table of Contents

Preface

When teaching a complex and ever-changing discipline such as information security, students are best served by beginning with a high-level understanding of the subject before they tackle the details. A solid grasp of the objectives, terminology, principles, and frameworks will help them understand how to place issues in a proper context for determining working solutions. That is the goal of this text: to introduce students to the most important topics of information security and pique their interest to learn more.

The body of knowledge (as it is called in the IT security industry) is vast, deep, and, at times, baffling. Solutions are not always straightforward because the problems they address are rarely intuitive. No cookbook or universal recipe for IT security success exists. Ideally, protecting computer systems from attacks and unauthorized access means anticipating problems and devising strategies to address how people, processes, and technologies interact. The goal, although not always realistic, is to prevent these problems from happening instead of simply reacting to them as so many organizations do today.

This is rarely easy.

This book navigates the ocean of information technology (IT) security issues while keeping the technical jargon to a minimum. Chapters are ordered to follow the major “domains” of the Common Body of Knowledge, to help prepare students for a more detailed examination of the topics, if that is their desire.

If you decide to enter the field of information security, you’ll find this book helpful in charting your course in joining the ranks of professionals and specialists in information security.

About the Authors

Mark Merkow, CISSP, CISM, CSSLP, is a technical director for a Fortune 100 financial services firm, where he works on implementing and operating a software security practice for the enterprise. He has more than 35 years of IT experience, including 20 years in IT security. Mark has worked in a variety of roles, including applications development, systems analysis and design, security engineering, and security management. Mark holds a master's degree in decision and info systems from Arizona State University (ASU), a master's of education in Distance Learning from ASU, and a bachelor's degree in Computer Info Systems from ASU.

Jim Breithaupt is a data integrity manager for a major bank, where he manages risk for a large data mart. He has more than 30 years of data processing experience and has co-authored several other books on information systems and information security, along with Mark Merkow.

Acknowledgments

From Mark Merkow:

To begin, I'm deeply grateful to my friend and co-author, Jim, who has an amazing ability to turn the obscure into the transparent. Without Jim, there would be no book.

Thanks to my wife, Amy Merkow, as always, for her positive attitude, full support, and unwavering belief in the written word.

I also want to thank our far-scattered children, Josh Merkow, Jasmine Merkow, Brandon Bohlman, and Caitlyn Bohlman, for their support throughout the writing process.

Tremendous thanks goes to Betsy Brown, Tonya Simpson, and the entire staff at Pearson, along with Jeff Riley at Box Twelve Communications, for their commitment to excellence, efficiency, and positive attitude, all of which make working with them a total pleasure.

Special thanks goes to my agent, Carole Jelen at Waterside Productions, for the remarkable effort that goes into book contracting and publication.

From Jim Breithaupt:

First, I would like to thank Mark Merkow for being the guiding light of every writing project he has asked me to share with him. If it weren't for Mark's extensive knowledge of data processing and his enthusiasm for our endeavors, this book, like all the others, would never have come to fruition. I would also like to acknowledge Margaret and my children, Faye and Bo, who are my joy and inspiration. Finally, I'd like to give a tip of the hat to Carole Jelen with Waterside Productions for her assistance, and to the fine technical reviewers and editors at Pearson for helping make this book possible.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: feedback@pearsonitcertification.com

Mail: Pearson IT Certification
ATTN: Reader Feedback
800 East 96th Street
Indianapolis, IN 46240 USA

Reader Services

Visit our website and register this book at www.pearsonitcertification.com/register for convenient access to any updates, downloads, or errata that might be available for this book.

This page intentionally left blank

This page intentionally left blank

Chapter 2

Information Security Principles of Success

Chapter Objectives

After reading this chapter and completing the exercises, you will be able to do the following:

- Build an awareness of 12 generally accepted basic principles of information security to help you determine how these basic principles apply to real-life situations
- Distinguish among the three main security goals
- Learn how to design and apply the principle of defense in depth
- Comprehend human vulnerabilities in security systems to better design solutions to counter them
- Explain the difference between functional requirements and assurance requirements
- Comprehend the fallacy of security through obscurity to avoid using it as a measure of security
- Comprehend the importance of risk-analysis and risk-management tools and techniques for balancing the needs of business
- Determine which side of the open disclosure debate you would take

Introduction

Many of the topics information technology students study in school carry directly from the classroom to the workplace. For example, new programming and systems analysis and design skills can often be applied on new systems-development projects as companies espouse cloud computing and mobile infrastructures that access internal systems.

Security is a little different. Although their technical skills are certainly important, the best security specialists combine their practical knowledge of computers and networks with general theories about security, technology, and human nature. These concepts, some borrowed from other fields, such as military defense, often take years of (sometimes painful) professional experience to learn. With a conceptual and principled view of information security, you can analyze a security need in the right frame of reference or context so you can balance the needs of permitting access against the risk of allowing such access. No two systems or situations are identical, and no cookbooks can specify how to solve certain security problems. Instead, you must rely on principle-based analysis and decision making.

This chapter introduces these key information security principles, concepts, and durable "truths."

Principle 1: There Is No Such Thing As Absolute Security

In 2003, the art collection of the Whitworth Gallery in Manchester, England, included three famous paintings by Van Gogh, Picasso, and Gauguin. Valued at more than $7 million, the paintings were protected by closed-circuit television (CCTV), a series of alarm systems, and 24-hour rolling patrols. Yet in late April 2003, thieves broke into the museum, evaded the layered security system, and made off with the three masterpieces. Several days later, investigators discovered the paintings in a nearby public restroom along with a note from the thieves saying, "The intention was not to steal, only to highlight the woeful security."

The burglars' lesson translates to the information security arena and illustrates the first principle of information security (IS): Given enough time, tools, skills, and inclination, a malicious person can break through any security measure. This principle applies to the physical world as well and is best illustrated with an analogy of safes or vaults that businesses commonly use to protect their assets. Safes are rated according to their resistance to attacks using a scale that describes how long it could take a burglar to open them. They are divided into categories based on the level of protection they can deliver and the testing they undergo. Four common classes of safe ratings are B-Rate, C-Rate, UL TL-15, and UL TL-30:

- **B-Rate:** B-Rate is a catchall rating for any box with a lock on it. This rating describes the thickness of the steel used to make the lockbox. No actual testing is performed to gain this rating.
- **C-Rate:** This is defined as a variably thick steel box with a 1-inch-thick door and a lock. No tests are conducted to provide this rating, either.
- **UL TL-15:** Safes with an Underwriters Laboratory (UL) TL-15 rating have passed standardized tests as defined in UL Standard 687 using tools and an expert group of safe-testing engineers. The UL TL-15 label requires that the safe be constructed of 1-inch solid steel or equivalent. The label means that the safe has been tested for a net working time of 15 minutes using "common hand tools, drills, punches hammers, and pressure applying devices." *Net working time* means that when the tool comes off the safe, the clock stops. Engineers exercise more than 50 different types of attacks that have proven effective for safecracking.

- **UL TL-30:** UL TL-30 testing is essentially the same as the TL-15 testing, except for the net working time. Testers get 30 minutes and a few more tools to help them gain access. Testing engineers usually have a safe's manufacturing blueprints and can disassemble the safe before the test begins to see how it works.

FYI: Confidentiality by Another Name

Confidentiality is sometimes referred to as the principle of least privilege, meaning that users should be given only enough privilege to perform their duties, and no more. Some other synonyms for confidentiality you might encounter include *privacy*, *secrecy*, and *discretion*.

As you learn in Chapter 5, "Security Architecture and Design," security testing of hardware and software systems employs many of the same concepts of safe testing, using computers and custom-developed testing software instead of tools and torches. The outcomes of this testing are the same, though: As with software, no safe is burglar proof; security measures simply buy time. Of course, buying time is a powerful tool. Resisting attacks long enough provides the opportunity to catch the attacker in the act and to quickly recover from the incident. This leads to the second principle.

FYI: Confidentiality Models

Confidentiality models are primarily intended to ensure that no unauthorized access to information is permitted and that accidental disclosure of sensitive information is not possible. Common confidentiality controls are user IDs and passwords.

Principle 2: The Three Security Goals Are Confidentiality, Integrity, and Availability

All information security measures try to address at least one of three goals:

- Protect the confidentiality of data
- Preserve the integrity of data
- Promote the availability of data for authorized use

These goals form the confidentiality, integrity, availability (CIA) triad, the basis of all security programs (see Figure 2.1). Information security professionals who create policies and procedures (often referred to as governance models) must consider each goal when creating a plan to protect a computer system.

FIGURE 2.1 The CIA triad.

FYI: CIA Triad

The principle of information security protection of confidentiality, integrity, and availability cannot be overemphasized: This is central to all studies and practices in IS. You'll often see the term *CIA triad* to illustrate the overall goals for IS throughout the research, guidance, and practices you encounter.

Integrity Models

Integrity models keep data pure and trustworthy by protecting system data from intentional or accidental changes. Integrity models have three goals:

- Prevent unauthorized users from making modifications to data or programs
- Prevent authorized users from making improper or unauthorized modifications
- Maintain internal and external consistency of data and programs

An example of integrity checks is balancing a batch of transactions to make sure that all the information is present and accurately accounted for.

Availability Models

Availability models keep data and resources available for authorized use, especially during emergencies or disasters. Information security professionals usually address three common challenges to availability:

- Denial of service (DoS) due to intentional attacks or because of undiscovered flaws in implementation (for example, a program written by a programmer who is unaware of a flaw that could crash the program if a certain unexpected input is encountered)
- Loss of information system capabilities because of natural disasters (fires, floods, storms, or earthquakes) or human actions (bombs or strikes)
- Equipment failures during normal use

Some activities that preserve confidentiality, integrity, and/or availability are granting access only to authorized personnel, applying encryption to information that will be sent over the Internet or stored on digital media, periodically testing computer system security to uncover new vulnerabilities, building software defensively, and developing a disaster recovery plan to ensure that the business can continue to exist in the event of a disaster or loss of access by personnel.

Principle 3: Defense in Depth as Strategy

A bank would never leave its assets inside an unguarded safe alone. Typically, access to the safe requires passing through layers of protection that might include human guards and locked doors with special access controls. Furthermore, the room where the safe resides could be monitored by closed-circuit television, motion sensors, and alarm systems that can quickly detect unusual activity. The sound of an alarm might trigger the doors to automatically lock, the police to be notified, or the room to fill with tear gas.

Layered security, as in the previous example, is known as defense in depth. This security is implemented in overlapping layers that provide the three elements needed to secure assets: prevention, detection, and response. Defense in depth also seeks to offset the weaknesses of one security layer by the strengths of two or more layers.

In the information security world, defense in depth requires layering security devices in a series that protects, detects, and responds to attacks on systems. For example, a typical Internet-attached network designed with security in mind includes routers, firewalls, and intrusion detection systems (IDS) to protect the network from would-be intruders; employs traffic analyzers and real-time human monitors who watch for anomalies as the network is being used to detect any breach in the layers of protection; and relies on automated mechanisms to turn off access or remove the system from the network in response to the detection of an intruder.

Finally, the security of each of these mechanisms must be thoroughly tested before deployment to ensure that the integrated system is suitable for normal operations. After all, a chain is only as good as its weakest link.

In Practice

Phishing for Dollars

Phishing is another good example of how easily intelligent people can be duped into breaching security. Phishing is a dangerous Internet scam, and is becoming increasingly dangerous as targets are selected using data available from social media and enable a malicious person to build a profile of the target to better convince him the scam is real. A phishing scam typically operates as follows:

- The victim receives an official-looking email message purporting to come from a trusted source, such as an online banking site, PayPal, eBay, or other service where money is exchanged, moved, or managed.
- The email tells the user that his or her account needs updating immediately or will be suspended within a certain number of days.
- The email contains a URL (link) and instructs the user to click on the link to access the account and update the information. The link text appears as though it will take the user to the expected site. However, the link is actually a link to the attacker's site, which is made to look exactly like the site the user expects to see.
- At the spoofed site, the user enters his or her credentials (ID and password) and clicks Submit.
- The site returns an innocuous message, such as "We're sorry—we're unable to process your transaction at this time," and the user is none the wiser.
- At this point, the victim's credentials are stored on the attacker's site or sent via email to the perpetrator, where they can be used to log in to the *real* banking or exchange site and empty the account before the user knows what happened.

Phishing and resultant ID theft and monetary losses are on the increase and will begin to slow only after the cycle is broken through awareness and education. Protect yourself by taking the following steps:

- Look for telltale signs of fraud: Instead of addressing you by name, a phishing email addresses you as "User" or by your email address; a legitimate message from legitimate companies uses your name as they know it.
- Do not click on links embedded in unsolicited finance-related email messages. A link might look legitimate, but when you click on it, you could be redirected to the site of a phisher. If you believe that your account is in jeopardy, type in the known URL of the site in a new browser window and look for messages from the provider after you're logged in.
- Check with your provider for messages related to phishing scams that the company is aware of. Your bank or other financial services provider wants to make sure you don't fall victim and will often take significant measures to educate users on how to prevent problems.

Principle 4: When Left on Their Own, People Tend to Make the Worst Security Decisions

The primary reason identity theft, viruses, worms, and stolen passwords are so common is that people are easily duped into giving up the secrets technologies use to secure systems. Organizers of Infosecurity Europe, Britain's biggest information technology security exhibition, sent researchers to London's Waterloo Station to ask commuters to hand over their office computer passwords in exchange for a free pen. Three-quarters of respondents revealed the information immediately, and an additional 15 percent did so after some gentle probing. Study after study like this one shows how little it takes to convince someone to give up their credentials in exchange for trivial or worthless goods.

Principle 5: Computer Security Depends on Two Types of Requirements: Functional and Assurance

Functional requirements describe what a system *should* do. Assurance requirements describe how functional requirements should be implemented and tested. Both sets of requirements are needed to answer the following questions:

- Does the system do the right things (behave as promised)?
- Does the system do the right things in the right way?

These are the same questions that others in noncomputer industries face with verification and validation. Verification is the process of confirming that one or more predetermined requirements or specifications are met. Validation then determines the correctness or quality of the mechanisms used to meet the needs. In other words, you can develop software that addresses a need, but it might contain flaws that could compromise data when placed in the hands of a malicious user.

Consider car safety testing as an example. Verification testing for seat belt functions might include conducting stress tests on the fabric, testing the locking mechanisms, and making certain the belt will fit the intended application, thus completing the functional tests. Validation, or assurance testing, might then include crashing the car with crash-test dummies inside to "prove" that the seat belt is indeed safe when used under normal conditions and that it can survive under harsh conditions.

With software, you need both verification and validation answers to gain confidence in products before launching them into a wild, hostile environment such as the Internet. Most of today's commercial off-the-shelf (COTS) software and systems stop at the first step, verification, without bothering to test for obvious security vulnerabilities in the final product. Developers of software generally lack the wherewithal and motivation needed to try to break their own software. More often, developers test that the software meets the specifications in each function that is present but usually do not try to find ways to circumvent the software and make it fail. You learn more about security testing of software in Chapter 5.

Principle 6: Security Through Obscurity Is Not an Answer

Many people in the information security industry believe that if malicious attackers don't know how software is secured, security is better. Although this might seem logical, it's actually untrue. Security through obscurity means that hiding the details of the security mechanisms is sufficient to secure the system alone. An example of security through obscurity might involve closely guarding the written specifications for security functions and preventing all but the most trusted people from seeing it. Obscuring security leads to a false sense of security, which is often more dangerous than not addressing security at all.

If the security of a system is maintained by keeping the implementation of the system a secret, the entire system collapses when the first person discovers how the security mechanism works—and someone is always determined to discover these secrets. The better bet is to make sure no one mechanism is responsible for the security of the entire system. Again, this is defense in depth in everything related to protecting data and resources.

In Chapter 11, "Cryptography," you'll see how this principle applies and why it makes no sense to keep an algorithm for cryptography secret when the security of the system should rely on the cryptographic keys used to protect data or authenticate a user. You can also see this in action with the open-source movement: Anyone can gain access to program (source) code, analyze it for security problems, and then share with the community improvements that eliminate vulnerabilities and/or improve the overall security through simplification (see Principle 9).

Principle 7: Security = Risk Management

It's critical to understand that spending more on securing an asset than the intrinsic value of the asset is a waste of resources. For example, buying a $500 safe to protect $200 worth of jewelry makes no practical sense. The same is true when protecting electronic assets. All security work is a careful balance between the level of risk and the expected reward of expending a given amount of resources. Security is concerned not with eliminating all threats within a system or facility, but with eliminating known threats and minimizing losses if an attacker succeeds in exploiting a vulnerability. Risk analysis and risk management are central themes to securing information systems. When risks are well understood, three outcomes are possible:

- The risks are mitigated (countered).
- Insurance is acquired against the losses that would occur if a system were compromised.
- The risks are accepted and the consequences are managed.

Risk assessment and risk analysis are concerned with placing an economic value on assets to best determine appropriate countermeasures that protect them from losses.

The simplest form of determining the degree of a risk involves looking at two factors:

- What is the consequence of a loss?
- What is the likelihood that this loss will occur?

Figure 2.2 illustrates a matrix you can use to determine the degree of a risk based on these factors.

	Consequences				
Likelihood	1. Insignificant	2. Minor	3. Moderate	4. Major	6. Catastrophic
A (almost certain)	High	High	Extreme	Extreme	Extreme
B (likely)	Moderate	High	High	Extreme	Extreme
C (moderate)	Low	Moderate	High	Extreme	Extreme
D (unlikely)	Low	Low	Moderate	High	Extreme
E (rare)	Low	Low	Moderate	High	High

FIGURE 2.2 Consequences/likelihood matrix for risk analysis.

After determining a risk rating, one of the following actions could be required:

- **Extreme risk:** Immediate action is required.
- **High risk:** Senior management's attention is needed.
- **Moderate risk:** Management responsibility must be specified.
- **Low risk:** Management is handled by routine procedures.

In the real world, risk management is more complicated than simply making a human judgment call based on intuition or previous experience with a similar situation. Recall that every system has unique security issues and considerations, so it's imperative to understand the specific nature of data the system will maintain, what hardware and software will be used to deploy the system, and the security skills of the development teams. Determining the likelihood of a risk coming to life requires understanding a few more terms and concepts:

- Vulnerability
- Exploit
- Attacker

Vulnerability refers to a known problem within a system or program. A common example in InfoSec is called the buffer overflow or buffer overrun vulnerability. Programmers tend to be trusting and not worry about who will attack their programs, but instead worry about who will use their programs legitimately. One feature of most programs is the capability for a user to "input" information or requests. The program instructions (source code) then contain an "area" in memory (buffer) for these inputs and act upon them when told to do so. Sometimes the programmer doesn't check to see if the input is proper or innocuous. A malicious user, however, might take advantage of this weakness and overload the input area with more information than it can handle, crashing or disabling the program. This is called buffer overflow, and it can permit a malicious user to gain control over the system. This common vulnerability with software must be addressed when developing systems. Chapter 13, "Software Development Security," covers this in greater detail.

An exploit is a program or "cookbook" on how to take advantage of a specific vulnerability. It might be a program that a hacker can download over the Internet and then use to search for systems that contain the vulnerability it's designed to exploit. It might also be a series of documented steps on how to exploit the vulnerability after an attacker finds a system that contains it.

An attacker, then, is the link between a vulnerability and an exploit. The attacker has two characteristics: skill and will. Attackers either are skilled in the art of attacking systems or have access to tools that do the work for them. They have the will to perform attacks on systems they do not own and usually care little about the consequences of their actions.

In applying these concepts to risk analysis, the IS practitioner must anticipate who might want to attack the system, how capable the attacker might be, how available the exploits to a vulnerability are, and which systems have the vulnerability present.

Risk analysis and risk management are specialized areas of study and practice, and the IS professionals who concentrate in these areas must be skilled and current in their techniques. You can find more on risk management in Chapter 4, "Governance and Risk Management."

Principle 8: The Three Types of Security Controls Are Preventative, Detective, and Responsive

Controls (such as documented processes) and countermeasures (such as firewalls) must be implemented as one or more of these previous types, or the controls are not there for the purposes of security. Shown in another triad, the principle of defense in depth dictates that a security mechanism serve a purpose by preventing a compromise, detecting that a compromise or compromise attempt is underway, or responding to a compromise while it's happening or after it has been discovered.

Referring to the example of the bank vault in Principle 3, access to a bank's safe or vault requires passing through layers of protection that might include human guards and locked doors with special access controls (prevention). In the room where the safe resides, closed-circuit televisions, motion sensors, and alarm systems quickly detect any unusual activity (detection). The sound of an alarm could trigger the doors to automatically lock, the police to be notified, or the room to fill with tear gas (response).

These controls are the basic toolkit for the security practitioner who mixes and matches them to carry out the objectives of confidentiality, integrity, and/or availability by using people, processes, or technology (see Principle 11) to bring them to life.

In Practice

How People, Process, and Technology Work in Harmony

To illustrate how people, process, and technology work together to secure systems, let's take a look a how the security department grants access to users for performing their duties. The process, called user access request, is initiated when a new user is brought into the company or switches department or role within the company. The user access request form is initially completed by the user and approved by the manager.

When the user access request is approved, it's routed to information security access coordinators to process using the documented procedures for granting access. After access is granted and the process for sharing the user's ID and password is followed, the system's technical access control system takes over. It protects the system from unauthorized access by requiring a user ID and password, and it prevents password guessing from an unauthorized person by limiting the number of attempts to three before locking the account from further access attempts.

In Practice

To Disclose or Not to Disclose—That Is the Question!

Having specific knowledge of a security vulnerability gives administrators the knowledge to properly defend their systems from related exploits. The ethical question is, how should that valuable information be disseminated to the good guys while keeping it away from the bad guys? The simple truth is, you can't really do this. Hackers tend to communicate among themselves far better than professional security practitioners ever could. Hackers know about most vulnerabilities long before the general public gets wind of them. By the time the general public is made aware, the hacker community has already developed a workable exploit and disseminated it far and wide to take advantage of the flaw before it can be patched or closed down.

Because of this, open disclosure benefits the general public far more than is acknowledged by the critics who claim that it gives the bad guys the same information.

Here's the bottom line: If you uncover an obvious problem, raise your hand and let someone who can do something about it know. If you see something, say something. You'll sleep better at night!

Principle 9: Complexity Is the Enemy of Security

The more complex a system gets, the harder it is to secure. With too many "moving parts" or interfaces between programs and other systems, the system or interfaces become difficult to secure while still permitting them to operate as intended. You learn in Chapter 5 how complexity can easily get in the way of comprehensive testing of security mechanisms.

Principle 10: Fear, Uncertainty, and Doubt Do Not Work in Selling Security

At one time, "scaring" management into spending resources on security to avoid the unthinkable was effective. The tactic of fear, uncertainty, and doubt (FUD) no longer works: Information security and IT management is too mature. Now IS managers must justify all investments in security using techniques of the trade. Although this makes the job of information security practitioners more difficult, it also makes them more valuable because of management's need to understand what is being protected and why. When spending resources can be justified with good, solid business rationale, security requests are rarely denied.

Principle 11: People, Process, and Technology Are All Needed to Adequately Secure a System or Facility

As described in Principle 3, "Defense in Depth as Strategy," the information security practitioner needs a series of countermeasures and controls to implement an effective security system. One such control might be dual control, a practice borrowed from the military. The U.S. Department of Defense uses a dual control protocol to secure the nation's nuclear arsenal. This means that at least two on-site people must agree to launch a nuclear weapon. If one person were in control, he or she could make an error in judgment or act maliciously for whatever reason. But with dual control, one person acts as a countermeasure to the other: Chances are less likely that both people will make an error in judgment or act maliciously. Likewise, no one person in an organization should have the ability to control or close down a security activity. This is commonly referred to as separation of duties.

Process controls are implemented to ensure that different people can perform the same operations exactly in the same way each time. Processes are documented as procedures on how to carry out an activity related to security. The process of configuring a server operating system for secure operations is documented as one or more procedures that security administrators use and can be verified as done correctly.

Just as the information security professional might establish process controls to make sure that a single person cannot gain complete control over a system, you should never place all your faith in technology. Technology can fail, and without people to notice and fix technical problems, computer

systems would stall permanently. An example of this type of waste is installing an expensive firewall system (a network perimeter security device that blocks traffic) and then turning around and opening all the ports that are intended to block certain traffic from entering the network.

People, process, and technology controls are essential elements of several areas of practice in information technology (IT) security, including operations security, applications development security, physical security, and cryptography. These three pillars of security are often depicted as a three-legged stool (see Figure 2.3).

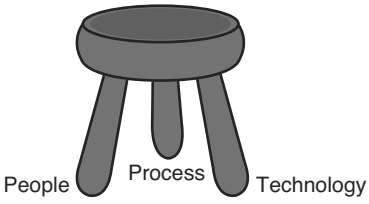

FIGURE 2.3 The people, process, and technology triad.

Principle 12: Open Disclosure of Vulnerabilities Is Good for Security!

A raging and often heated debate within the security community and software developing centers concerns whether to let users know about a problem before a fix or patch can be developed and distributed. Principle 6 tells us that security through obscurity is not an answer: Keeping a given vulnerability secret from users and from the software developer can only lead to a false sense of security. Users have a right to know about defects in the products they purchase, just as they have a right to know about automobile recalls because of defects. The need to know trumps the need to keep secrets, to give users the right to protect themselves.

Summary

To be most effective, computer security specialists not only must know the technical side of their jobs, but also must understand the principles behind information security. No two situations that security professionals review are identical, and there are no recipes or cookbooks on universal security measures. Because each situation calls for a distinct judgment to address the specific risks inherent in information systems, principles-based decision making is imperative. An old saying goes, "If you only have a hammer, every problem looks like a nail." This approach simply does not serve today's businesses, which are always striving to balance risk and reward of access to electronic records. The goal is to help you create a toolkit and develop the skills to use these tools like a master craftsman. Learn these principles and take them to heart, and you'll start out much further along than your peers who won't take the time to bother learning them!

As you explore the rest of the Common Body of Knowledge (CBK) domains, try to relate the practices you find to one or more of these. For example, Chapter 8, "Physical Security Control," covers physical security, which addresses how to limit access to physical spaces and hardware to authorized personnel. This helps prevent breaches in confidentiality, integrity, and availability, and implements the principle of defense in depth. As you will find, these principles are mixed and matched to describe why certain security functions and operations exist in the real world of IT.

Test Your Skills

MULTIPLE CHOICE QUESTIONS

1. Which of the following represents the three goals of information security?

   A. Confidentiality, integrity, and availability

   B. Prevention, detection, and response

   C. People controls, process controls, and technology controls

   D. Network security, PC security, and mainframe security

2. Which of the following terms best describes the assurance that data has not been changed unintentionally due to an accident or malice?

   A. Availability

   B. Confidentiality

   C. Integrity

   D. Auditability

3. Related to information security, confidentiality is the opposite of which of the following?

   A. Closure
   B. Disclosure
   C. Disaster
   D. Disposal

4. The CIA triad is often represented by which of the following?

   A. Triangle
   B. Diagonal
   C. Ellipse
   D. Circle

5. Defense in depth is needed to ensure that which three mandatory activities are present in a security system?

   A. Prevention, response, and prosecution
   B. Response, collection of evidence, and prosecution
   C. Prevention, detection, and response
   D. Prevention, response, and management

6. Which of the following statements is true?

   A. The weakest link in any security system is the technology element.
   B. The weakest link in any security system is the process element.
   C. The weakest link in any security system is the human element.
   D. Both B and C

7. Which of the following best represents the two types of IT security requirements?

   A. Functional and logical
   B. Logical and physical
   C. Functional and assurance
   D. Functional and physical

8. Security functional requirements describe which of the following?

   A. What a security system should do by design
   B. What controls a security system must implement
   C. Quality assurance description and testing approach
   D. How to implement the system

9. Which of the following statements is true?

   A. Security assurance requirements describe how to test the system.

   B. Security assurance requirements describe how to program the system.

   C. Security assurance requirements describe to what degree the testing of the system is conducted.

   D. Security assurance requirements describe implementation considerations.

10. Which of the following terms best describes the probability that a threat to an information system will materialize?

   A. Threat

   B. Vulnerability

   C. Hole

   D. Risk

11. Which of the following terms best describes the absence or weakness in a system that may possibly be exploited?

   A. Vulnerability

   B. Threat

   C. Risk

   D. Exposure

12. Which of the following statements is true?

   A. Controls are implemented to eliminate risk and eliminate the potential for loss.

   B. Controls are implemented to mitigate risk and reduce the potential for loss.

   C. Controls are implemented to eliminate risk and reduce the potential for loss.

   D. Controls are implemented to mitigate risk and eliminate the potential for loss.

13. Which of the following terms best describes a cookbook on how to take advantage of a vulnerability?

   A. Risk

   B. Exploit

   C. Threat

   D. Program

14. Which of the following represents the three types of security controls?

    A. People, functions, and technology
    B. People, process, and technology
    C. Technology, roles, and separation of duties
    D. Separation of duties, processes, and people

15. Which of the following statements is true?

    A. Process controls for IT security include assignment of roles for least privilege.
    B. Process controls for IT security include separation of duties.
    C. Process controls for IT security include documented procedures.
    D. All of the above

EXERCISES

EXERCISE 2.1: Understanding the Importance of Information Confidentiality

Why is confidentiality important to corporate information? What kinds of abuses can you think of in the absence of controls on confidentiality? What criminal activities could be reduced or eliminated if confidentiality controls were effectively implemented?

EXERCISE 2.2: Evaluating Real-World Defense in Depth

Find some analogies to the principle of defense in depth in the physical world, and make some diagrams of the mechanism you locate. Consider how a bank implements defense in depth and how corporations protect themselves from intruders entering their buildings.

EXERCISE 2.3: Avoiding Security Through Obscurity

Why is security through obscurity a bad idea for the overall security of a system?

EXERCISE 2.4: Identifying a Phishing Scam

Go to www.opendns.com/phishing-quiz/ and take the "Think You Can Outsmart Internet Scammers?" quiz. How well did you perform at identifying phishing scams?

EXERCISE 2.5: Evaluating Risk Management

Every day, you make risk-management decisions in your daily life. Should you get in the car and drive to the store? Should you jaywalk or cross at the light? Should you get on that airplane? Think about the risk-management decisions you make when using your PC:

1. What kinds of judgments do you make before downloading a piece of software?
2. What kinds of judgments do you make before writing an email to your boss?
3. What mental steps do you go through before taking some action?

PROJECTS

PROJECT 2.1: Understanding Email-Borne Viruses

1. Visit one or more of the antivirus software developer sites (Symantec, MacAfee, Computer Associates, Trend Micro, and so forth), and see if you can identify which viruses and worms require a user to click on an email attachment to replicate.
2. Trace the sophistication of the virus writers over time, and try to determine how they circumvent any improvements in user awareness of and education toward preventing viruses from spreading.

PROJECT 2.2: Researching Hackers

Open disclosure of software vulnerabilities is often associated with gray-hat hackers, described as security researchers who aren't particular about who learns about their findings. Research the three types of hackers (white hat, gray hat, and black hat), and try to determine their typical positions on full disclosure of software problems before patches or new versions of the software are made available in the marketplace. Use Google or your favorite Internet search engine with a query of "Open Disclosure of Software Vulnerabilities" to help you formulate your answers.

PROJECT 2.3: Comparing Physical and Virtual Risk-Management Techniques

1. How is risk management for physical systems similar to risk management for computer systems?
2. How are the two different?
3. What skill sets are required for each type?

This page intentionally left blank

Index

Symbols

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X – Z