Second Edition

CISSP GUIDE TO SECURITY ESSENTIALS

Peter H. Gregory

INFORMATION SECURITY PROFESSIONAL

CISSP Guide to Security Essentials

Second Edition

Peter H. Gregory

CENGAGE Learning

Australia • Brazil • Mexico • Singapore • United Kingdom • United States

CISSP Guide to Security Essentials

CISSP Guide to Security Essentials

Second Edition

Peter H. Gregory

CENGAGE Learning®

Australia • Brazil • Mexico • Singapore • United Kingdom • United States

CENGAGE Learning®

CISSP Guide to Security Essentials, Second Edition
Peter H. Gregory

SVP, GM Skills & Global Product Management: Dawn Gerrain
Product Development Manager: Leigh Hefferon
Senior Content Developer: Julia Leroux-Lindsey
Product Assistant: Scott Finger
Vice President, Marketing Services: Jennifer Ann Baker
Marketing Director: Michele McTighe
Marketing Manager: Eric La Scola
Marketing Coordinator: Will Guiliani
Senior Production Director: Wendy Troeger
Production Manager: Patty Stephan
Senior Content Project Manager: Brooke Greenhouse
Art Director: GEX Publishing Services
Cover Photo: © iStockPhoto.com/Henrik5000

Library of Congress Control Number: 2014949536

ISBN-13: 978-1-285-06042-2

ISBN-10: 1-285-06042-3

Cengage Learning
20 Channel Center Street
Boston, MA 02210
USA

Cengage Learning is a leading provider of customized learning solutions with office locations around the globe, including Singapore, the United Kingdom, Australia, Mexico, Brazil, and Japan. Locate your local office at: **www.cengage.com/global**

Cengage Learning products are represented in Canada by Nelson Education, Ltd.

To learn more about Cengage Learning, visit **www.cengage.com**

Purchase any of our products at your local college store or at our preferred online store **www.cengagebrain.com**

Printed in the United States of America
Print Number: 01 Print Year: 2014

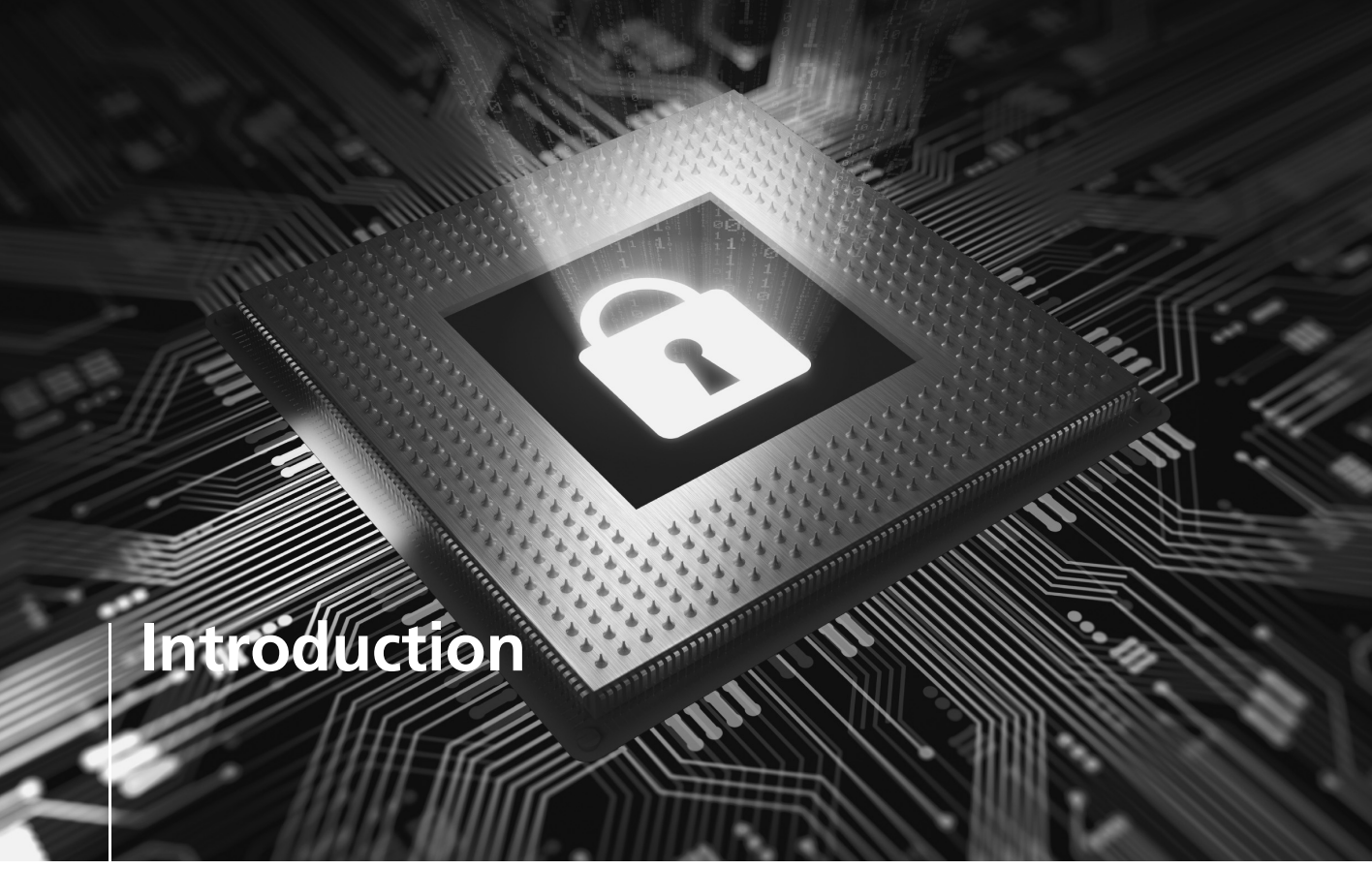
To Rebekah and Shannon, and to the memory of my son and daughters.

Brief Table of Contents

Table of Contents

CHAPTER 5

CHAPTER 10



Introduction

"If the Internet were a city street, I would not travel it in daylight," laments a chief information security officer for a prestigious university.

The Internet is critical infrastructure supporting the world's commerce, industrial control systems, and the daily lives of over a billion people. Cybercrime is escalating; once the domain of hackers and script kiddies, cyber-gangs, and organized criminal organizations have developed business opportunities for extortion, embezzlement, and fraud that surpasses income from illegal sex and drug trafficking. Criminals are going for the gold, the information held in information systems that are easily accessed and compromised anonymously from the Internet.

The information security industry is unable to keep up. Cybercriminals and hackers always seem to be at least one step ahead, and new threats and vulnerabilities crop up at a rate that exceeds our ability to continue protecting our most vital information and systems. Like other sectors in IT, security planners, analysts, engineers, and operators are expected to do more with less. Cybercriminals have never had it so good.

There are not enough good security professionals to go around. As a profession, information security in all its forms is relatively new. Fifty years ago there were perhaps a dozen information security professionals, and their jobs consisted primarily of making sure the doors were locked and that keys were issued only to personnel who had an established need for access. Today, whole sectors of industries are doing virtually all of their business online, and other critical infrastructures such as public utilities are controlled online via the Internet. The rate of growth in the information security

profession is falling way behind the rate of growth of critical information and infrastructures going online. This is making it all the more critical for today's and tomorrow's information security professionals to have a good understanding of the vast array of principles, practices, technologies, and tactics that are required to protect an organization's assets.

The CISSP (Certified Information Systems Security Professional) is easily the most recognized security certification in the information security industry. CISSP is also one of the most difficult certifications to earn, because it requires knowledge in almost every nook and cranny of information technology and physical security. The CISSP is a jack-of-all-trades certification that, like that of a general practitioner physician, makes us ready for nearly any threat that could come along.

The required body of knowledge for the CISSP certification is published and updated regularly. This book covers all of the material in the published body of knowledge, with each chapter clearly mapping to each of the ten categories within that body of knowledge.

With the demand for security professionals at an all-time high, whether you are a security professional in need of a reference, an IT professional with your sights on the CISSP certification, or a course instructor, *CISSP Guide to Security Essentials* has arrived just in time.

Intended Audience

This book is written for students and professionals who want to expand their knowledge of computer, network, and business security. It is not necessary that the reader specifically target CISSP certification; while this book is designed to support that objective, the student or professional who desires to learn more about security, but who does not aspire to earn the CISSP certification at this time, will benefit from this book as equally as a CISSP candidate.

CISSP Guide to Security Essentials is also ideal for someone in a self-study program. The end of each chapter has not only study questions, but also Hands-On Projects and Case Projects that you can do on your own with a computer running Windows, MacOS, or Linux.

The structure of this book is designed to correspond with the ten domains of knowledge for the CISSP certification, called the Common Body of Knowledge (CBK). While this alignment will be helpful for the CISSP candidate who wants to align her study with the CBK, this is not a detriment to other readers. This is because the CBK domains align nicely with professional practices such as access control, cryptography, physical security, and other sensibly organized categories.

This book's pedagogical features will help all readers who wish to broaden their skills and experience in computer and business security. Each chapter contains several Hands-On Projects that guide the reader through several key security activities, many of which are truly hands-on with computers and networks. Each chapter also contains Case Projects that take the reader into more advanced topics to help them apply the concepts in the chapter.

Chapter Descriptions

Here is a summary of the topics covered in each chapter of this book:

Chapter 1, "Information Security and Risk Management," begins with the fundamentals of information and business security—security and risk management—by explaining how an

organization's security program needs to support the organization's goals and objectives. The chapter continues with risk management, security management and strategies, personnel security, and professional ethics.

Chapter 2, "**Access Controls,**" discusses access control principles and architectures, and continues with descriptions of the types of attacks that are carried out against access control systems. The chapter also discusses how an organization can test its access controls to make sure they are secure.

Chapter 3, "**Software Development Security,**" begins with a discussion of the types of operating systems and application software, application models, and technologies. The chapter continues by exploring threats to software and countermeasures to deal with them. It explores how to secure the software development life cycle—the process used for the creation and maintenance of software. The chapter discusses software environment and security controls, and concludes with a discussion of the security of databases and data warehouses.

Chapter 4, "**Business Continuity and Disaster Recovery,**" explores the concepts and practices in business continuity planning and disaster recovery planning. The chapter provides a lengthy discourse on a practical approach to running a BCP / DRP project. Next, the chapter describes several approaches to testing BCP and DRP plans, and how such plans are maintained over time.

Chapter 5, "**Cryptography,**" begins with an introduction to the science of cryptography, the practice of hiding data in plain sight. The chapter continues with a discussion of the applications and uses of cryptography, and on the methodologies used by cryptographic algorithms. The chapter also includes a discussion of cryptography and key management.

Chapter 6, "**Legal, Regulations, Compliance, and Investigations,**" starts with a discussion of the different types of computer crime and the various ways that computers are involved in criminal activity. The next discussion focuses on the types and categories of laws in the U.S. and other countries, with a particular focus on computer-related laws. The chapter continues with a discussion of security incident response, investigations, and computer forensics, and concludes with a discussion of ethical issues in the workplace.

Chapter 7, "**Security Operations,**" introduces and discusses the broad topic of putting security controls, concepts, and technologies into operation in an organization. The specific topics discussed includes records management, backup, anti-virus, remote access, administrative access, resource protection, incident management, vulnerability management, change management, and configuration management. The chapter discusses resource protection, high-availability application architectures, and attacks and countermeasures for IT operations.

Chapter 8, "**Physical and Environmental Security,**" begins with a discussion of site access controls for the physical protection of worksites that may include IT systems. The chapter discusses secure siting, which is the process of identifying risk factors associated with the location and features of an office building. The chapter provides an overview of fire prevention and suppression, theft prevention, and building environmental controls including electric power and heating, ventilation, and air conditioning.

Chapter 9, "**Security Architecture and Design,**" discusses security models that have been developed and are still in use from the 1970s to the present. The chapter continues with a discussion of information system evaluation models including the Common Criteria. The chapter discusses computer hardware architecture and computer software, including operating systems, tools, utilities, and applications. Security threats and countermeasures in the context of computer software are also explored.

Chapter 10, "**Telecommunications and Network Security,**" is a broad exploration of telecommunications and network technologies. The chapter examines the TCP/IP and OSI protocol models, and continues with a dissection of the TCP/IP protocol suite. The chapter addresses TCP/IP network architecture, protocols, addressing, devices, routing, authentication, access control, tunneling, and services. The chapter concludes with a discussion of network-based threats and countermeasures.

Appendix A, "**The Ten Domains of CISSP Security,**" provides a background on the CISSP certification, and then describes the ten domains in the CISSP Common Body of Knowledge.

Appendix B, "**The (ISC)^2 Code of Ethics,**" contains the full text of the (ISC)^2 Code of Ethics, which every CISSP candidate is required to support and uphold. The Code of Ethics is a set of enduring principles to guide the behavior of every security professional.

Appendix C, "**The CISSP Certification,**" describes the certification qualifications, the exam registration process, and the certification exam itself. The chapter includes tips to help the reader establish a study plan. Requirements for maintaining the CISSP certification are discussed.

Glossary lists common information security and risk management terms that are found in this book.

Features

To aid you in fully understanding computer and business security, this book includes many features designed to enhance your learning experience.

- **Maps to the CISSP Common Body of Knowledge (CBK).** The material in this text covers all of the CISSP exam objectives. Aside from Information Security and Risk Management being addressed first in the book, the sequence of the chapters follows the ten CISSP domains.
- **Common Body of Knowledge objectives included.** Each chapter begins with the precise language from the (ISC)^2 Common Body of Knowledge for the respective topic in the CISSP certification. This helps to remind the reader of the CISSP certification requirements for that particular topic.
- **Chapter Objectives.** Each chapter begins with a detailed list of the concepts to be mastered within that chapter. This list provides you with both a quick reference to the chapter's contents and a useful study aid.
- **Illustrations and Tables.** Numerous illustrations of security vulnerabilities, attacks, and defenses help you visualize security elements, theories, and concepts. In addition,

the many tables provide details and comparisons of practical and theoretical information.

- **Chapter Summaries.** Each chapter's text is followed by a summary of the concepts introduced in that chapter. These summaries provide a helpful way to review the ideas covered in each chapter.
- **Key Terms.** All of the terms in each chapter that were introduced with bold text are gathered in a Key Terms list with definitions at the end of the chapter, providing additional review and highlighting key concepts.
- **Review Questions.** The end-of-chapter assessment begins with a set of review questions that reinforce the ideas introduced in each chapter. These questions help you evaluate and apply the material you have learned. Answering these questions will ensure that you have mastered the important concepts and provide valuable practice for taking the CISSP exam.
- **Hands-On Projects.** Although it is important to understand the theory behind network security, nothing can improve upon real-world experience. To this end, each chapter provides several Hands-On Projects aimed at providing you with practical security software and hardware implementation experience. These projects can be completed on Windows 7 or Windows 8 (and, in many cases, Windows XP, MacOS, Linux). Some will use software downloaded from the Internet.
- **Case Projects.** Located at the end of each chapter are several Case Projects. In these extensive exercises, you implement the skills and knowledge gained in the chapter through real analysis, design, and implementation scenarios.
- **$(ISC)^2$ Code of Ethics.** The entire $(ISC)^2$ Code of Ethics is included at the end of this book. It is this author's opinion that the security professional's effectiveness in the workplace is a direct result of one's professional ethics and conduct.

Text and Graphic Conventions

Wherever appropriate, additional information and exercises have been added to this book to help you better understand the topic at hand. Icons throughout the text alert you to additional materials. The icons used in this textbook are described below.

The Note icon draws your attention to additional helpful material related to the subject being described.

Hands-On Projects in this book are preceded by the Hands-On icon and descriptions of the exercises that follow.

Case Project icons mark Case Projects, which are scenario-based assignments. In these extensive case examples, you are asked to implement independently what you have learned.

Instructor's Materials

The following additional materials are available when this book is used in a classroom setting. All of the supplements available with this book are provided for download at our Instructor Companion Site. Simply search for this text at *login.cengage.com*.

Electronic Instructor's Manual—The Instructor's Manual that accompanies this textbook provides additional instructional material to assist in class preparation, including suggestions for lecture topics, suggested lab activities, tips on setting up a lab for the hands-on assignments, and solutions to all end-of-chapter materials.

Cognero(R) Cengage Learning Testing Powered by Cognero is a flexible, online system that allows you to author, edit, and manage test bank content from multiple Cengage Learning solutions; create multiple test versions in an instant; and deliver tests from your LMS, your classroom or wherever you want.

PowerPoint Presentations—This book comes with a set of Microsoft PowerPoint slides for each chapter. These slides are meant to be used as a teaching aid for classroom presentations, to be made available to students on the network for chapter review, or to be printed for classroom distribution. Instructors are also at liberty to add their own slides to cover additional topics.

Practice Questions—250 sample exam questions are included.

Notes About This Edition

This is the second edition of this book. The second edition of this book was produced for three primary reasons:

- Six years will have passed since publication of the first edition. There have been changes and advances in security practices and security technologies in the intervening five years.
- $(ISC)^2$ completed a significant update to the CISSP Common Body of Knowledge (CBK), reflecting these same changes in security technologies and practices.
- $(ISC)^2$ has made fundamental changes to its CISSP exam, changing it from paper based to computer based. The locations where candidates take the CISSP exam have also changed.

Acknowledgments

First, I want to thank my wife and best friend, Rebekah. Without her patience and support, writing this book could not have been possible.

It takes a team of professionals to produce a teaching book. Those with whom I worked directly are mentioned here.

Several individuals at Cengage Learning have also been instrumental in the production of this book. First, Product Manager Nick Lombardi established the scope and direction for this book. Senior Content Developer Julia Leroux-Lindsey managed the author through the entire writing, reviewing, and production process, keeping track of the details as the author sent in chapter files, images, and other materials. Next, Senior Content Project Manager Brooke Baker kept track of the details as the author sent in chapter files, images, and other

materials. Manuscript Quality Assurance tester Serge Palladino ensured that the text was free from errors. Certainly there were others: editors, compositors, graphic artists, who were also involved in this book project. Heartfelt thanks to all of you.

Special recognition goes to the book's technical reviewers. These are industry and academic subject matter experts who carefully read through the manuscript to make sure that it is both technically accurate and also well organized, with accurate and understandable descriptions and explanations. This book's technical reviewers are:

- Dr. Barbara Endicott-Popovsky, the Director for the Center of Information Assurance and Cybersecurity at the University of Washington, designated by the NSA as a Center for Academic Excellence in Information Assurance Education.
- Michael Simon, a leading expert in computer security, information assurance, and security policy development. Mike and I have also written two books together.
- John Sanderson at St. Clair College in Windsor, who provided valuable and thoughtful feedback in several important areas.
- Guy Garrett at Gulf Coast State College, whose insight challenged me to go the extra mile on several technical explanations.

Special thanks to Kirk Bailey for his keen insight over the years and for fighting the good fight.

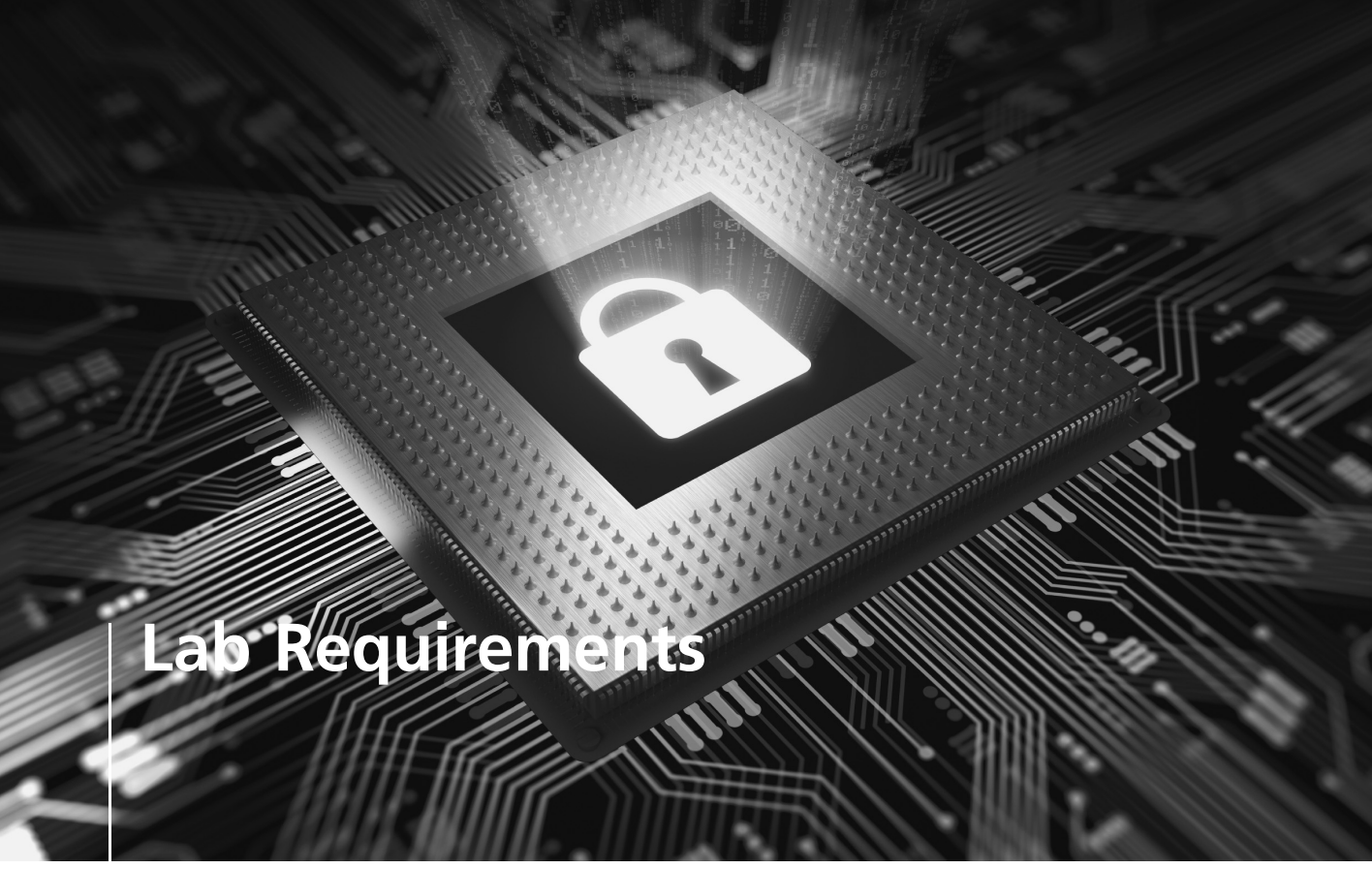
I am honored to have had the opportunity work with this outstanding and highly professional group of individuals at Cengage Learning, together with the reviewers and others of you who never compromised on the pursuit of excellence.

About the Author

Peter H. Gregory, CISSP, CISA, CRISC, CCSK, PCI-QSA, is the author of over thirty books on information security and technology, including *CISA All-In-One Study Guide, IT Disaster Recovery Planning For Dummies, Biometrics For Dummies,* and *Solaris Security*. He has spoken at numerous security conferences, including RSA, SecureWorld Expo, InfraGard, and the West Coast Security Forum.

Peter is a Director of Strategic Services at FishNet Security, the leading provider of information security solutions that combine technology, services, support and training. He is the lead instructor and advisory board member for the University of Washington's certificate program in information security, and an advisory board member and guest lecturer for the University of Washington's certificate program in information security and risk management. He is a graduate of the FBI Citizens Academy.

In his free time he enjoys the outdoors in Washington State with his wife and family.



Lab Requirements

To the User

This book contains numerous hands-on lab exercises, many of which require a personal computer and, occasionally, specialized software.

Information and business security is not just about the technology; it's also about people, processes, and the physical facility in which all reside. For this reason, some of the labs do not involve the exploration of some aspect of computers or networks, but instead are concerned with business requirements, analysis, or critical evaluation of information. But even in these non-technical labs, a computer with word processing, spreadsheet, or illustration software will be useful for collecting and presenting information.

Hardware and Software Requirements

These are all of the hardware and software requirements needed to perform the end-of-chapter Hands-On Projects:

- Windows 7 or Windows 8 (in some projects, Windows XP, MacOS, or a current Linux distribution are sufficient)
- An Internet connection and Web browser (e.g., Firefox or Internet Explorer)
- Anti-virus software

Specialized Requirements

The need for specialized hardware or software is kept to a minimum. However, the following chapters do require specialized hardware or software:

- Chapter 2: Zone Labs' Zone Alarm firewall, or Comodo Firewall
- Chapter 3: Secunia Personal Software Inspector (PSI), IBM AppScan
- Chapter 10: Notebook or desktop computer with Wi-Fi NIC compatible with the Vistumbler tool

Free Downloadable Software Is Required in the Following Chapters

Chapter 2:

- Zone Labs' Zone Alarm firewall or Comodo Firewall
- WinZip version 9 or newer

Chapter 3:

- Secunia Personal Software Inspector (PSI)
- Microsoft Threat Analysis & Modeling tool

Chapter 5:

- TrueCrypt
- GnuPG
- OpenStego
- WinZip version 9 or newer

Chapter 9:

- Microsoft Process Explorer
- NMAP

Chapter 10:

- Wireshark
- NMAP
- Vistumbler

chapter 1

Information Security and Risk Management

Topics in This Chapter:

- How Security Supports Organizational Mission, Goals, and Objectives
- Risk Management
- Security Management
- Personnel Security

The *International Information Systems Security Certification Consortium* (ISC)^2 *Common Body of Knowledge* (CBK) defines the key areas of knowledge for Information Security Governance and Risk Management in this way:

The Information Security Governance and Risk Management domain entails the identification of an organization's information assets and the development, documentation, implementation and updating of policies, standards, procedures and guidelines that ensure confidentiality, integrity, and availability. Management tools such as data classification, risk assessment, and risk analysis are used to identify the threats, classify assets, and to rate their vulnerabilities so that effective security measures and controls can be implemented.

The candidate is expected to understand the planning, organization, roles and responsibilities of individuals in identifying and securing an organization's information assets; the development and use of policies stating management's views and position on particular topics and the use of guidelines, standards, and procedures to support the policies; security training to make employees aware of the importance of information security, its significance, and the specific security-related requirements relative to their position; the importance of confidentiality, proprietary and private information; third-party management and service level agreements related to information security; employment agreements; employee hiring and termination practices; and risk management practices and tools to identify, rate, and reduce the risk to specific resources.

Key areas of knowledge:

- *Understand and align security function to goals, mission, and objectives of the organization*
- *Understand and apply security governance*
- *Understand and apply concepts of confidentiality, integrity, and availability*
- *Develop and implement security policy*
- *Manage the information life cycle (e.g., classification, categorization, and ownership)*
- *Manage third-party governance (e.g., on-site assessment, document exchange and review, process/policy review)*
- *Understand and apply risk management concepts*
- *Manage personnel security*
- *Develop and manage security education, training, and awareness*
- *Manage the security function*

Even though this domain is positioned as number 3 in the Certified Information Systems Security Professional (CISSP) common body of knowledge, it is placed first in this book because all security activities should take place as a result of security and risk management processes.

Organizational Purpose

In order to protect an organization's assets, it is first necessary to understand several basic characteristics of the organization, including its goals, mission, and objectives. All of these are statements that define what the organization desires to achieve and how it will proceed to achieve them. These three terms are described in more detail as follows:

Mission

The mission of an organization is a statement of its ongoing purpose and reason for existence. An organization usually publishes its mission statement, so that its stakeholders, including employees, customers, suppliers, shareholders, and owners, share a common understanding of the organization's stated purpose. Some example mission statements:

> *"Support and provide members and constituents with credentials, resources, and leadership to secure information and deliver value to society."*—(ISC)²
>
> *"Global cryptologic dominance through responsive presence and network advantage."*—United States National Security Agency
>
> *"Organize the world's information and make it universally accessible and useful."*—Google
>
> *"Facebook's mission is to give people the power to share and make the world more open and connected."*—Facebook

As security professionals, we need to be aware of our organization's mission, because it will, in part, influence how we will approach the need to protect the organization's assets.

Objectives

Objectives clearly define the results an organization and its managers want to achieve in a specific time frame. Objectives reflect the broader purposes given by the mission statement and provide specific, observable, and measurable outcomes. Stakeholders periodically review the organization's results by comparing them to the objectives. This process determines the success of the organization and its management. Objectives state strategic priorities. When these are distilled into specific, achievable steps, they become goals.

Sample organization objectives include:

> *"Become the world's leading business human capital management company."*
>
> *"Reduce delayed flight departures to less than 5% of all scheduled flights."*
>
> *"Achieve the lowest personnel turnover in field sales."*

Security personnel need to understand and use the organization's objectives to guide their plans. Security often impedes activities needed to achieve objectives. Achieving the proper balance between security and operations requires evaluating threats through the lens of risk. The optimum solution allows employees to reach goals and achieve the organization's objectives with a minimum amount of risk to confidential data.

Goals

While objectives describe desired outcomes for an organization, goals specify specific accomplishments that will enable the organization to meet its objectives.

Some sample organization goals are:

> *"Obtain ISO 27001 certification by the end of third quarter."*
>
> *"Reduce development costs by twenty percent in the next fiscal year."*
>
> *"Complete the integration of CRM and ERP systems by the end of November."*

Security Support of Mission, Objectives, and Goals

Security professionals support an organization's mission, objectives, and goals by developing processes, practices, and procedures for protecting assets. They assess threats and develop mitigation steps in the context of probability, or risk, that a potential threat can occur. Effective security policy requires including this important consideration in every significant organizational decision. *Forbes* cited a PricewaterhouseCoopers survey showing a significant increase in employment of chief security officers. The report indicated that 41 percent of companies employed a CSO compared to 27 percent one year earlier. Employment of chief information security officers rose from 29 to 44 percent (Greenberg, 2008). Security programs fail without executive support, and the presence of security professionals in the organization's highest management levels reflects the growing importance of this field.

This is discussed in greater detail later in this chapter in the Security Management section.

Risk Management

Risk management is the process of minimizing potential losses. Even though a potential for loss always exists, many can be minimized or avoided. In the event a loss occurs, risk management practices determine how to reduce the costs. Since the potential for loss always exists, the key is to determine the probability or level of risk from a potential threat, scenario, or activity and determine its acceptability. Risk assessment techniques determine the level of risk and determine if the level of risk exceeds an organization's risk tolerance. In that case, the next step requires the development of a strategy to ameliorate specific risks in order to achieve an acceptable level of overall risk to the organization. In the vernacular this means: find the level of risk (associated with a given activity or asset) and improve if needed.

The National Institute of Standards and Technology (NIST) defines four risk management processes—framing, assessing, monitoring, and responding—in Special Publication 800-39. NIST develops security standards for U.S. government agencies, and these publications often assist private-sector organizations with risk management planning.

Risk Management Principles

Risk Assessment

Risk assessments are activities that are carried out to discover, describe, analyze, and evaluate risks. Risk assessments may be qualitative, quantitative, or a combination of these.

Internal audit is related to risk assessment; internal audit is discussed in a separate section in this chapter.

Qualitative Risk Assessment A qualitative risk assessment occurs with a predefined scope of **assets** or activities. Assets can, for example, consist of software applications, information systems, business equipment, business processes, or buildings. Activities may consist of actions or tasks carried out by an individual, group, or department.

A qualitative risk assessment collects descriptive information, including information that cannot be reduced to measurable values. It will typically identify a number of characteristics about an asset or activity, including:

- *Classification*. Assets may be classified according to risk level, business function, or the sensitivity or criticality of data stored or processed by an asset.
- ***Vulnerabilities***. These are weaknesses in design, configuration, documentation, procedure, or implementation.
- ***Threats***. These are potential activities that would, if they occurred, exploit specific vulnerabilities and result in a security incident.
- *Threat probability*. An expression of the likelihood that a specific threat will be carried out, usually expressed in a Low-Medium-High or simple numeric (1–5 or 1–10) scale. In a qualitative risk assessment, this is not a numeric probability but an arbitrary ranking of probability, as a way of distinguishing low probability from high probability.
- *Impact*. An expression of the influence upon the organization if a threat was carried out.
- ***Countermeasures***. These are actual or proposed measures that reduce the risk associated with vulnerabilities or threats.

Here is an example. A security manager is performing a qualitative risk assessment on assets in an IT environment. For each asset, the manager builds a chart that lists each threat, along with the probability of realization. The chart might resemble the list in Table 1-1.

This is an oversimplified example, but sometimes qualitative risk analysis won't be much more complicated than this—although a real risk analysis should list many more threats and countermeasures.

Quantitative Risk Assessment Although qualitative criteria do provide guidance for assessing and evaluating risks, quantitative assessments treat these conditions as discrete mathematical valuations. Often quantitative risks produce stronger arguments for security policies and encourage leaders to support aggressive implementation of security controls. A quantitative risk assessment can be thought of as an extension of a qualitative risk assessment.

Threat	Impact	Probability	Countermeasure	Probability with Countermeasure
Flooding	H	L	Water alarms	L
Theft	H	L	Key card, video surveillance, guards	L
Earthquake	M	M	Lateral rack bracing; attach all assets to racks	L
Logical intrusion	H	M	Network-based intrusion detection system; host-based intrusion detection system	L

Table 1-1 Risk assessment chart

A quantitative risk assessment will include the elements of a qualitative risk assessment but will contain additional items, including:

- *Asset value*. Usually this is a dollar figure that may represent the replacement cost of an asset, but it could also represent income derived through the use of the asset.
- ***Exposure factor (EF)***. The proportion of an asset's value that is likely to be lost through a particular threat, usually expressed as a percentage. Another way to think about exposure factor is to consider the *impact* of a specific threat on an asset.
- ***Single loss expectancy (SLE)***. This is the cost of a single loss through the single event realization of a particular threat. This is a result of the calculation:

$$\text{SLE} = \text{asset value (\$)} \times \text{exposure factor (\%)}$$

- ***Annualized rate of occurrence (ARO)***. This is the probability that a loss will occur in a year's time. This is usually expressed as a percentage, which can be greater than 100% if it is believed that a loss can occur more than once per year.
- *Annual loss expectancy (ALE)*. This is the yearly estimate of loss of an asset, calculated as follows:

$$\text{ALE} = \text{ARO} \times \text{SLE}$$

Let's look at an example: an organization asset, an executive's laptop computer that is worth $2,000. The asset value is $2,000.

Now we will calculate the exposure factor (EF), which is the proportion of the laptop's value that is lost through a particular threat. The threat of theft will, of course, result in the entire laptop's value to be lost. For theft, EF = 100%. For sake of example, let's add another threat, that of damage, if the executive drops the laptop and breaks the screen. For that threat, the EF = 50% (presuming a $1,000 repair bill to replace the LCD screen).

For theft, the single loss expectancy (SLE) is $2,000 × 100% = $2,000. For damage, the SLE is $2,000 × 50% = $1,000.

Now we need to calculate how often either of these scenarios might occur in a single year. For theft, let us presume that there is a 10% probability that this executive's laptop will be stolen. Thus, the ARO = 10%. This particular executive is really clumsy and drops his laptop computer a lot, so the ARO for the threat of accidental damage is 25%.

The annual loss expectancy (ALE) for theft is 10% × $2,000 = $200.

The ALE for accidental damage is 25% × $1,000 = $250.

This all means that the organization may lose $450 ($200 for theft and $250 for damage) each year in support of the executive's laptop computer. Knowing this will help managers make more intelligent spending decisions for any protective measures that they feel will reduce the probability or impact of these and other threats. An example of such a measure is a remote wipe capability for laptop computers and smartphones.

Quantifying Countermeasures

Annual loss expectancy (**ALE**) is the cost that the organization is likely to bear through the loss or compromise of the asset. Because ALE is expressed in dollars (or other local currency), the organization can now make decisions

regarding specific investments in countermeasures that are designed to reduce the risk. The risk analysis can be extended to include the impact of countermeasures on the overall risk equation:

- *Costs of countermeasures*. Each countermeasure has a specific cost associated with it. This may be the cost of additional protective equipment, software, or labor costs.
- *Changes in exposure factor*. A specific countermeasure may have an impact on a specific threat. For example, the use of an FM-200-based fire extinguishment system will mean that a fire in a business location will cause less damage than a sprinkler-based extinguishment system, but it is more expensive to reload.
- *Changes in single loss expectancy*. Specific countermeasures may influence the probability that a loss will occur. For instance, the introduction of an advanced malware protection appliance will reduce the frequency of successful malware attacks.

Geographic Considerations Organizations can take quantitative risk analysis a step or two further by calculating SLE, ALE, and ARO values in specific geographic locations. This is useful in organizations with similar assets located in different locations where the probability of loss or the replacement cost of these assets varies enough to be identified.

Specific Risk Assessment Methodologies The risk assessment steps described in this section are purposely simplistic, with the intention of illustrating the concepts of identifying the value of assets and by using formulas to arrive at a quantitative figure that represents the probable loss or compromise of assets in a year's time. For some organizations, this simple approach may be sufficient. On the other hand, there are several formal approaches to risk assessment that may be suitable for larger or more complex efforts. Among these approaches are:

- *OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)*. Developed by Carnegie Mellon University's Software Engineering Institute (SEI), OCTAVE is an approach where analysts identify assets and their criticality, identify vulnerabilities and threats, evaluate risks, and create a protection strategy to reduce risk.
- *FRAP (Facilitated Risk Analysis Process)*. This is a qualitative risk analysis methodology that can be used to prescreen a subject of analysis as a means to determine whether a full-blown quantitative risk analysis is needed.
- *Spanning Tree Analysis*. This can be thought of as a visual method for identifying categories of risks, as well as specific risks, using the metaphor of a tree and its branches. This approach would be similar to a Mind Map for identifying categories and specific threats and/or vulnerabilities.
- NIST 800-30, *Risk Management Guide for Information Technology Systems*. This document describes a formal approach to risk assessment that includes threat and vulnerability identification, control analysis, impact analysis, and a matrix depiction of risk determination and control recommendations.

Risk Treatment

When a qualitative or quantitative risk assessment is performed, an organization's management can begin the process of determining what steps, if any, can be taken to manage the risks identified in the risk assessment. The four general approaches to risk treatment are:

- Risk acceptance
- Risk avoidance
- Risk mitigation
- Risk transfer

It is important to remember that the objective of risk treatment is typically not to eliminate risk—often risk cannot be completely eliminated, but only managed.

Risk Avoidance The associated activity that introduces the risk is discontinued. For instance, an organization performs a risk analysis of an Internet-based shopping cart application, and then decides to abandon the use of the application altogether. This is **risk avoidance**.

Risk Mitigation This involves the use of countermeasures to reduce the risks initially identified in the risk analysis. Examples of **risk reduction** in information systems include firewalls, intrusion detection systems, access reviews, and DMZ networks.

Risk Acceptance In a typical risk assessment, there will be many identified risks, typically ranked as high, medium, and low risk. In an organization with scarce resources, management may choose to forego mitigation of all of the risks ranked low, in other words leaving things as they are and accepting the stated risks. This is known as **risk acceptance**. Occasionally, medium and high risks will also be accepted, although such a decision usually requires more thoughtful consideration as well as formal management approval.

Risk Transfer **Risk transfer** typically involves the use of insurance as a means for mitigating risk. For instance, a risk analysis on the use of laptop computers may identify theft as one risk. While the organization may mitigate the risk through the use of cable locks, it may transfer part of the risk to an insurance company. Note that risk transfer usually involves a cost (insurance premiums) that should be considered in a quantitative risk analysis.

Residual Risk In any particular risk situation, generally only some of the risk can be avoided, reduced, or transferred. There is always some remaining risk, called **residual risk**. Typically this risk must be accepted, unless management can enact another round of analysis and a fresh set of countermeasures to avoid, reduce, or transfer the risk. But even then, there will typically be some "leftover" risk, called *residual risk*.

Security Management Concepts

As security moved from a task to a standalone professional discipline, practitioners developed a de facto framework of foundational concepts. These include:

- Security controls
- CIA Triad
- Defense in depth
- Single points of failure
- Fail open, fail closed, fail soft
- Privacy

The ISO 27001 standard, "Information Technology—Security Techniques—Information Security Management Systems—Requirements," is a respected standard for information security management. Originally developed as British Standard 7799, the standard was adopted by the International Standards Organization (ISO) in 2000. ISO 27001 was later updated in 2005. ISO 27001 is a top-down process approach to security management that requires continuous improvement in an organization's security management system.

Security Controls

Security controls are the measures that are taken to reduce risks through the origination and enforcement of **security policies**. The types of controls used are detective, deterrent, preventive, corrective, recovery, and compensating. These controls are discussed in detail in Chapter 3, "Software Development Security."

The CIA Triad

The core principles of information security are confidentiality, integrity, and availability, often coined as **CIA**. All other concepts and activities in information security are based on these principles. The CIA Triad is depicted in Figure 1-1.

Confidentiality The principle of confidentiality asserts that only properly authorized parties can access information and functions.

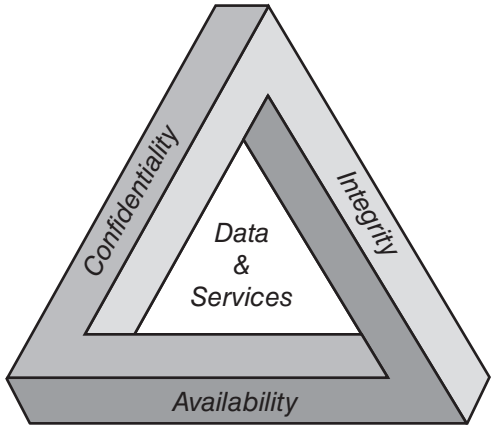


Figure 1-1 The CIA Triad