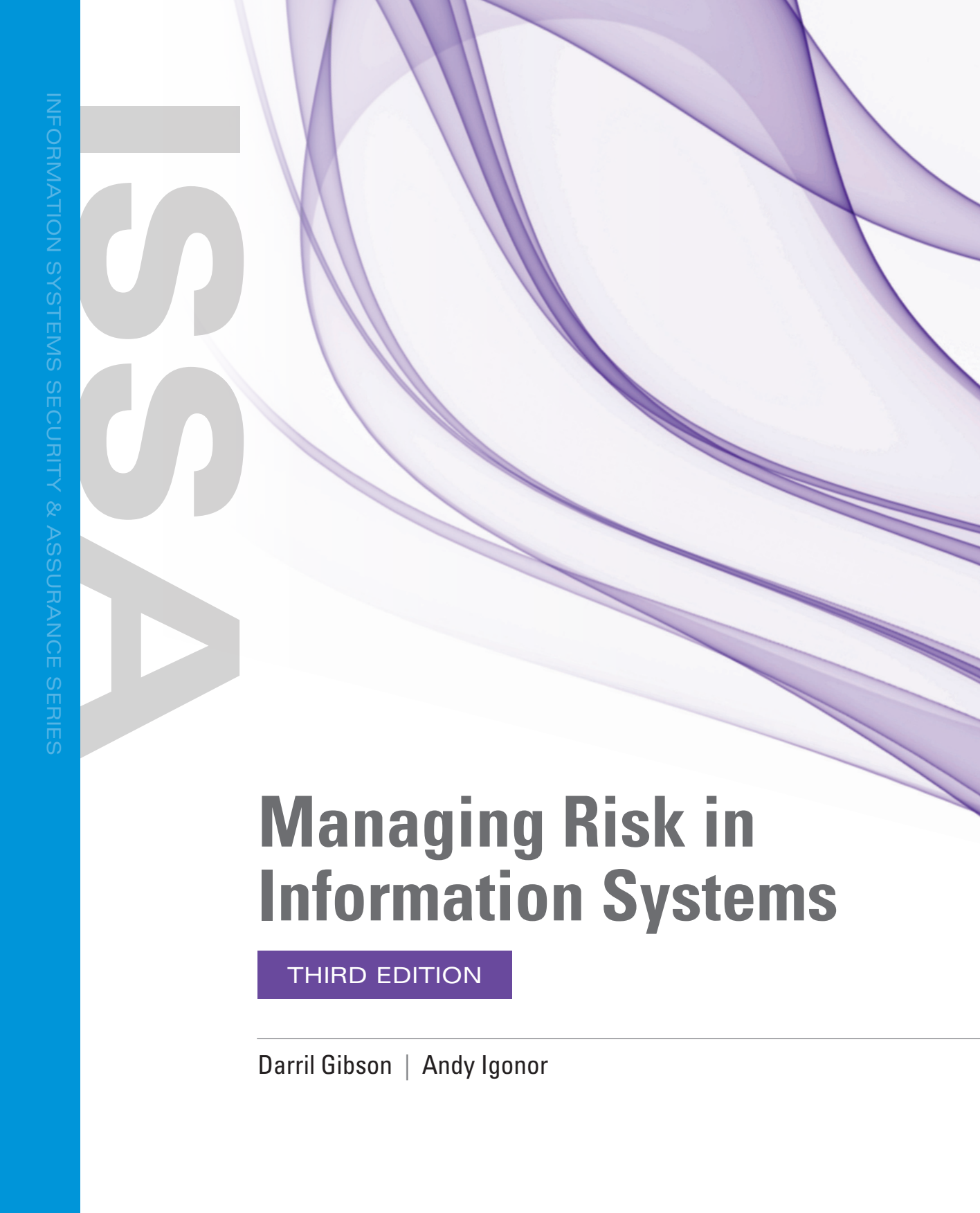


Managing Risk in Information Systems

THIRD EDITION

Darril Gibson | Andy Igonor

INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES

ISSA

Managing Risk in Information Systems

THIRD EDITION

Darril Gibson | Andy Igonor

JONES & BARTLETT
LEARNING

World Headquarters
Jones & Bartlett Learning
5 Wall Street
Burlington, MA 01803
978-443-5000
info@jblearning.com
www.jblearning.com

Jones & Bartlett Learning books and products are available through most bookstores and online booksellers. To contact Jones & Bartlett Learning directly, call 800-832-0034, fax 978-443-8000, or visit our website, www.jblearning.com.

Substantial discounts on bulk quantities of Jones & Bartlett Learning publications are available to corporations, professional associations, and other qualified organizations. For details and specific discount information, contact the special sales department at Jones & Bartlett Learning via the above contact information or send an email to specialsales@jblearning.com.

Production Credits
Math/CS team:
VP, Product Management: Christine Emerton
Director of Product Management: Laura Pagluica
Product Manager: Ned Hinman
Product Specialist/Assistant: Melissa Duffy
Product Coordinator: Paula-Yuan Gregory
Project Manager: Kristen Rogers
Senior Project Specialist: Alex Schab
Senior Digital Project Specialist: Angela Dooley
Marketing Manager: Michael Sullivan
Product Fulfillment Manager: Wendy Kilborn
Composition: Exela Technologies
Development Editor: Ginny Munroe
Technical Editor: Jeff Parker
Cover Design: Briana Yates
Text Design: Briana Yates
Senior Media Development Editor: Troy Liston
Media Development Editor: Faith Brosnan
Rights & Permissions Manager: John Rusk
Rights Specialist: James Fortney
Cover Image (Title Page, Part Opener, Chapter Opener): © Sai Chan/Shutterstock
Printing and Binding: LSC Communications

Library of Congress Cataloging-in-Publication Data
Library of Congress Cataloging-in-Publication Data unavailable at time of printing.

6048

Printed in the United States of America

25 24 23 22 21 10 9 8 7 6 5 4 3 2

Brief Contents

Contents

To my wife, who has enriched my life in so many ways over the past 22 years.
I'm looking forward to sharing many more with you.

—Darril Gibson

To my wife and our boys, for their patience and support.

—Andy Igonor

Preface

Purpose of This Book

This book is part of the Information Systems Security & Assurance Series from Jones & Bartlett Learning (https://www.jblearning.com/cybersecurity/issa). Designed for courses and curriculums in IT security, cybersecurity, information assurance, and information systems security, this series features a comprehensive, consistent treatment of the most current thinking and trends in this critical subject area. The books in this series deliver fundamental information security principles packed with real-world applications and examples. Authored by Certified Information Systems Security Professionals (CISSPs), they deliver comprehensive information on all aspects of information security. Reviewed word for word by leading technical experts in the field, these books are not just current, but also forward thinking, putting you in the position to solve the cybersecurity challenges not just of today, but of tomorrow as well.

This book provides a comprehensive view of managing risk in information systems. It covers the fundamentals of risk and risk management and includes in-depth details on more comprehensive risk management topics in three major parts.

Part One, Risk Management Business Challenges, addresses many of the issues relevant to present-day businesses. It covers details of risks, threats, and vulnerabilities. Topics help students understand the importance of risk management in the organization, including many of the techniques used to manage risks. Several current laws are presented with clear descriptions of how they are relevant in organizations. It also includes a chapter describing the contents of a risk management plan.

Part Two, Mitigating Risk, focuses on risk assessments. Topics presented include risk assessment approaches, including the overall steps in performing a risk assessment. It covers the importance of identifying assets and then identifying potential threats, vulnerabilities, and exploits against these assets. Chapter 9 covers the types of controls that can be used to mitigate risk. The last two chapters in this part identify how to plan risk mitigation throughout the organization and convert the risk assessment into a risk management plan.

Part Three, Risk Mitigation Plans, covers the many elements of risk mitigation plans, such as a business impact analysis and a business continuity plan. The last two chapters cover disaster recovery and computer incident response team plans.

Learning Features

The writing style of this book is practical and conversational. Step-by-step examples of information security concepts and procedures are presented throughout the text. Each chapter begins with a statement of learning objectives. Illustrations are used to clarify the material and vary the presentation. The text is sprinkled with Notes, Tips, FYIs, and sidebars to alert the reader to additional and helpful information related to the subject under discussion. Chapter Assessments appear at the end of each chapter, with solutions provided in the back of the book.

Chapter summaries are included in the text to provide a rapid review or preview of the material and to help students understand the relative importance of the concepts presented.

Audience

The material is suitable for undergraduate or graduate computer science or information science majors, students at a two-year technical college or community college who have a basic technical background, or readers who have a basic understanding of IT security and want to expand their knowledge.

New to This Edition

This text has been broadly updated to include new and emerging concepts in the expanding field of information systems and cybersecurity, in particular risk management. Concepts are more appropriately defined and explained; for example, the definition of *risk* references *assets* as a critical component of the totality of risk. Risk management and assessment topics have been updated throughout the book with references to threat sources, for example, advanced persistent threats. Included are updated references and examples of threat-likelihood impacts and how organizations compute risk loss scenarios. Explanations of business continuity plans, minimum business continuity objectives, disaster recovery plans, and recovery sites are updated. Several new guidelines have been introduced in the text to reflect advances in the field of cybersecurity. In particular, federal guidelines from the National Institute of Standards and Technology (NIST) and the Department of Homeland Security have been updated, with the inclusion of new NIST Special Publications: 800-183; 800-154; 800-153; 800-150; 800-84; 800-63 a, b, and c; 800-53 Rev. 5; 800-34; and 800-37.

The text includes updated references to the current organizational state of affairs in the field of cybersecurity, such as surveys of executives in the field, and references to the new and emerging topics of cloud computing, analytics, mobile computing, artificial intelligence, machine learning, robotic process automation, and blockchain. Besides updated information on the NIST Risk Management Framework, updates to the Common Vulnerabilities and Exposures (CVE) are included. The textbook now has updated references to U.S. and international compliance laws, including the Federal Information Security Modernization Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), and the EU's General Data Protection Regulation (GDPR). The Children's Online Privacy Protection Act (COPPA) is introduced as well as the Equifax data breach. The text

includes updated references to ISACA's Control Objectives for Information and Related Technologies (COBIT) 2019. Updated end-of-chapter questions are also included in the text.

Cloud Labs

This text is accompanied by Cybersecurity Cloud Labs. These hands-on virtual labs provide immersive mock IT infrastructures whereby students can learn and practice foundational cybersecurity skills as an extension of the lessons in this textbook. For more information or to purchase the labs, visit go.jblearning.com/gibson3e.

Acknowledgments

Jones & Bartlett Learning would personally like to thank all the people who reviewed the second edition of this book, whose feedback helped to shape this revision:

Michael D. Barker
Columbus State University

David Barnes
Penn State Altoona

Casey Cegielski
Auburn University

Shaun L. Gray
University of the Cumberlands

Dr. Wendi M. Kappers
Embry-Riddle Aeronautical University

Andrew Mangle
Bowie State University

Francis J. Monaco
Charter Oak State College

Andrew Morrow
Penn State University Harrisburg

Phoebe Tsai
Cedarville University

George J. Trawick
National Defense University

About the Authors

Darril Gibson is the CEO of YCDA, LLC (short for You Can Do Anything). He regularly writes and consults on a wide variety of security and technical topics and holds several certifications, including MCSE, MCDBA, MCSD, MCITP, ITIL v3, Security+, SSCP, and CISSP. He has authored or coauthored more than 30 books, including the best-selling *Security+: Get Certified, Get Ahead* series of books, and regularly blogs at http://blogs.getcertifiedgetahead.com.

Andy Igonor currently serves as the director of Academic Programs and the associate dean of Information Technology/Cloud Computing at Western Governor's University. He previously served as the dean of the Ross College of Business at Franklin University. He is an IT professional and entrepreneur with over 20 years of experience spanning several industries, from education to health care and consulting. He has worked and lived in Africa, Asia, Europe, the Middle East, and North America. Andy holds a doctorate in Information Systems from the Bristol Business School, United Kingdom. He also holds several certifications, including Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC), and Certified Professional in Health Information Management and Systems (CPHIMS). He has published several articles in information technology and also coauthored four books.

PART ONE

Risk Management Business Challenges

CHAPTER 1

Risk Management Fundamentals

RISK MANAGEMENT is essential to the success of every organization; an organization that takes no risks may not fail, but it cannot thrive. On the other hand, an organization that ignores risks may fail when only a single threat is exploited. Today, information technology (IT) and its systems contribute to the success of many organizations. However, IT and its systems have inherent risks that expose an organization to harm and therefore require proper management to prevent an organization's failure.

Effective risk management starts with understanding the assets that require protection and the threats and vulnerabilities that might affect them. A person builds on this knowledge by identifying ways to mitigate the risks. Risks can be mitigated by reducing vulnerabilities or the impact of the risks. Then, customized plans to mitigate risks in different areas of the company can be created. A company typically has several risk mitigation plans in place; however, it is important to note that risks cannot be completely eliminated.

This text will help the student build a solid foundation in risk management as it relates to information systems and cybersecurity. It serves as an introduction to a career in this field. Many of the topics presented in just a few paragraphs in this text can fill entire chapters or books. The more the student learns, the closer he or she will be to becoming an expert whom others seek out to solve their problems.

Chapter 1 Topics

This chapter covers the following topics and concepts:

- What risk is and its relationship to threat, vulnerability, and asset loss
- What the major components of risk to an IT infrastructure are
- What risk management is and how important it is to the organization
- What some risk identification techniques are
- What some risk management techniques are

Chapter 1 Goals

When you complete this chapter, you will be able to:

- Define risk
- Identify the major components of risk
- Describe the relationship among threats, vulnerabilities, assets, and impact of loss
- Define risk management
- Describe risk management's relationship with profitability and survivability
- Explain the relationship between the cost of loss and the cost of risk management
- Describe how risk is perceived by different roles within an organization
- Identify threats
- List the different categories of threats
- Describe techniques to identify vulnerabilities
- Identify and define risk management techniques
- Describe the purpose of a cost-benefit analysis (CBA)
- Define residual risk

What Is Risk?

Risk is the likelihood or probability that something unexpected is going to occur. This unexpected result could be either a gain or a loss. In the world of information security, most organizations focus on ways to guard against asset losses. Losses occur when a threat exposes a vulnerability that could harm an asset. Companies employ risk assessment strategies to differentiate severe risks from minor risks. When this is done properly, administrators and managers can make rational decisions about how to handle each risk they've identified.

Risk management is the practice of identifying, assessing, controlling, and mitigating risks. In this discussion, the key terms that a person will need to be familiar with are shown in the following list. Each term will be discussed in detail later in the chapter.

- **Threat**—A **threat** is any activity that represents a possible danger.
- **Vulnerability**—A **vulnerability** is a weakness.
- **Asset**—An **asset** is a thing of value worth protecting.

NOTE

NIST Special Publication 800-37 Rev. 2 provides a definition of risk: "Risk is a measure of the extent to which an entity is threatened by a potential circumstance or event. Risk is also a function of the adverse impacts that arise if the circumstance or event occurs, and the likelihood of occurrence. Types of risk include program risk; compliance/regulatory risk; financial risk; legal risk; mission/business risk; political risk; security and privacy risk (including supply chain risk); project risk; reputational risk; safety risk; strategic planning risk."

- **Impact of loss—Impact of loss** is a loss resulting in a compromise to business functions or assets.

> **NOTE**
> Threats and vulnerabilities are explored in much more depth later in this chapter.

Risks to a business can result in a loss that negatively affects the business and its core business functions. A business commonly tries to limit, or control, its exposure to risks. The overall goal is to reduce as much as possible the impact of losses that can occur from risk.

Compromise of Business Functions

Business functions are the activities a business performs to sell products or services. If any of these functions are negatively affected, the business won't be able to sell as many products or services. The business will earn less revenue, resulting in an overall loss.

Here are a few examples of business functions and possible compromises:

- Salespeople regularly call or email customers. If the capabilities of either phones or email are reduced, sales are reduced.
- An organization receives several emails that are unrelated to business functions, which temporarily clog up email space and make network resources unavailable. This situation is referred to as a **denial of service (DoS) attack**. When a DoS attack happens across the organization's network whereby the network receives emails from multiple sources, it is called a **distributed denial of service (DDoS) attack**.
- A website sells products on the Internet. If the website is attacked and fails, sales are lost.
- Authors write articles that must be submitted by a deadline to be published. If the author's computer becomes infected with a virus, the deadline passes, and the article's value is reduced.
- Analysts compile reports used by management to make decisions. Data is gathered from internal servers and Internet sources. If network connectivity fails, analysts won't have access to current data. Management could make decisions based on inaccurate information.
- A warehouse application is used for shipping products that have been purchased. It identifies what has been ordered, where the products need to be sent, and where the products are located. If the application fails, products aren't shipped on time.
- A person calls an organization pretending to have a legitimate purpose and attempts to trick someone in the organization into divulging personal or protected information. This form of impersonation, known as **social engineering**, can compromise the organization's business functions and lead to losses.

Demystifying Social Engineering

Social engineering is a common technique used to trick people into revealing sensitive information. Nathan Ford (aka Nate), in the TV show *Leverage*, planned an elaborate scheme targeting the greedy and corrupt in a classic example of social engineering. A social engineer doesn't just say "give me your secrets." Instead, the attacker uses techniques such as flattery and deception, often relying on the victim's willingness to be helpful.

A common technique used in vulnerability assessments is to ask employees to give their usernames and passwords. The request may come in the form of an email or a phone call or even person-to-person.

For example, when sending an email to request a username and password, the email may be modified so that it looks as if it's coming from an executive. The email adds a sense of urgency and may include a reference to an important project. For example, the users might receive the following email:

> From: CEO
>
> Subj: Project upgrade
>
> All,
>
> The XYZ project is at risk of falling behind. As you know, this is integral to our success in the coming year. We're having a problem with user authentication. We think it's because passwords may have special characters that aren't recognized.
>
> I need everyone to reply to this email with their username and password. We must complete this test today, so please respond as soon as you receive this email.
>
> Thanks for your assistance.

When employees are trained to protect their passwords, they usually recognize the risks and don't reply. However, it has been shown that, when employees aren't trained, as many as 70 percent of the employees may respond.

Because compromises to any of these business functions can result in a loss of revenue, all of them represent a risk. One of the tasks when considering risk is identifying the important functions for a business and ensuring that organizations provide necessary employee training to reduce their weakest links (i.e., people with limited knowledge of technology and security).

The importance of any business function is relative to the business. In other words, the failure of a website for one company may be catastrophic if all products and services are sold through the website. Another company may use its website only to provide hours of operation to its customers; therefore, the website's failure will have less impact on the business.

Threats, Vulnerabilities, Assets, and Impact

Earlier, key terms related to risk were introduced. Their relationship can now be seen. When a threat exploits a vulnerability to gain access to an asset, the threat could potentially result in a loss if the asset is compromised. The impact of the threat identifies the severity of that loss. It is important to note that not all assets are considered valuable. The greater the value attached to an asset, the greater the severity of the loss will be, making the need to put controls in place to prevent the loss from being greater.

Threats

A threat is any circumstance or event with the potential to cause a loss. A threat can also be thought of as any activity that represents a possible danger. Threats are always present and cannot be eliminated, but they can be controlled. Assets represent anything of value worth protecting.

Threats have independent probabilities of occurring that often are unaffected by an organization's action. As an example, an attacker may be an expert in attacking web servers

FIGURE 1-1
Security objectives for information and information systems.

hosted on Apache. There is very little a company can do to stop this attacker from trying to attack. However, the company can reduce or eliminate vulnerabilities to reduce the attacker's chances of success.

Threats can be thought of as attempts to exploit vulnerabilities that result in the loss of **confidentiality**, **integrity**, or **availability** of a business asset. The protection of confidentiality, integrity, and availability is a common security objective for information systems.

FIGURE 1-1 shows these three security objectives as a protective triangle. If any side of the triangle is breached or fails, security fails. In other words, risks to confidentiality, integrity, or availability represent potential loss to an organization. Because of this, a significant amount of risk management is focused on protecting these resources.

- **Confidentiality**—Preventing unauthorized disclosure of information. Data should be available only to authorized users. Loss of confidentiality occurs when data is accessed by someone who should not have access to it. Data is protected using access controls and encryption technologies.
- **Integrity**—Ensuring data or an IT system is not modified or destroyed. If data is modified or destroyed, it loses its value to the company. Hashing is often used to ensure integrity.
- **Availability**—Ensuring data and services are available when needed. IT systems are commonly protected using fault tolerance and redundancy techniques. Backups are used to ensure the data is retained even if an entire building is destroyed.

NOTE
Confidentiality, integrity, and availability are often referred to as the *security triad*, or the *C-I-A triad*.

Vulnerabilities

A vulnerability is a weakness. It could be a procedural, technical, or administrative weakness. It could be a weakness in physical, technical, or operational security. Just as all threats don't result in a loss, all vulnerabilities don't result in a loss. A loss to an asset occurs only when an attacker is able to exploit the vulnerability.

TIP
The method used to take advantage of a vulnerability can also be referred to as an **exploit**.

Vulnerabilities may exist because they've never been corrected. They can also exist if security is weakened either intentionally or unintentionally.

Considering a locked door used to protect a server room, a technician could intentionally unlock it to make it easier to access. If the door doesn't shut tight on its own, it could accidentally be left open. Either way, the server room and its contents become vulnerable.

Assets

A business asset is anything that has measurable value to a company. If an asset has the potential to lose value, it is at risk. Value is defined as the worth of an asset to a business.

Assets can have both tangible and intangible values. The **tangible value** is the actual cost of the asset and can be expressed in monetary terms, such as $5,000. The tangible assets of a business include its inventory, furniture, and machinery. Examples of tangible IT assets are:

- **Computer systems**—Servers, desktop PCs, and mobile computers
- **Network components**—Routers, switches, firewalls, and any other components necessary to keep the network running
- **Software applications**—Any application that can be installed on a computer system
- **Data**—Includes the large-scale databases that are integral to many businesses; also includes the data used and manipulated by each employee or customer

The **intangible value** is value that cannot be measured by cost, such as client confidence or company reputation. Generally acceptable accounting principles (GAAP) refer to client confidence as **goodwill**.

For example, a company sells products via a website, and it earns $5,000 an hour in revenue. The web server hosting the website fails and is down for two hours. The cost to repair it totals $1,000. What is the tangible loss?

- **Lost revenue**—$5,000 times two hours equals $10,000
- **Repair costs**—$1,000
- **Total tangible value**—$11,000

The intangible value isn't as easy to calculate but is still important. For example, a customer with an urgent need tried to make a purchase when the website was down. If the same product is available somewhere else, he or she may choose to purchase the product elsewhere. That experience may damage the organization's reputation in the eye of that customer, and, if the customer's experience with the other business is positive, the customer may go directly to the second company the next time he or she wants to purchase this product. The loss of this future business cannot be measured, which makes it intangible.

Intangible value includes:

- **Future lost revenue**—Any additional purchases customers make with another company are a loss to the company whose website was down.
- **Cost of gaining the customer**—Large sums of money are invested in attracting customers. A repeat customer is much easier to sell to than acquiring a new customer. If a company loses a customer, the company's investment is lost.
- **Customer influence**—Customers have friends, families, and business partners. They commonly share their experience with others, especially if the experience is exceptionally positive or negative.

- **Reputation**—Customers share their negative experience with others, so one customer's bad experience could potentially influence other current or potential customers to avoid future business transactions.

One of the early steps in risk management is associated with identifying the assets of a company and the assets' associated costs. This data is used to prioritize risks for different assets. Once a risk has been prioritized, identifying risk management processes to protect the asset becomes easier.

Impact

The impact is the amount of the loss, which can be expressed in monetary terms, such as $5,000. The value of hardware and software is often easy to determine. If a laptop is stolen, the purchase or replacement value can be used to determine the value of the stolen laptop. However, some losses aren't easy to determine. If that same laptop held data, the value of the data is hard to estimate.

Descriptive terms, instead of monetary terms, can be used to explain the impact of a loss. For example, losses can be described in relative terms, such as *high*, *medium*, or *low*, which helps an organization quantify the loss by describing the potential harm. The harm might be to operations, such as the inability to perform critical business functions; assets, such as hardware or facilities; individuals, such as loss of personal information, injury, or loss of life; other organizations, resulting in financial losses or damaged relationships; or the nation, affecting government operations or national security.

Published by the National Institute of Standards and Technology, the Guide for Conducting Risk Assessments (NIST SP 800-30) includes the following scale for assessing the impact of threats to the business's assets:

- **Very high**—Indicates multiple severe or catastrophic adverse effects. *Severe* or *catastrophic* indicates a loss of critical business functions. This loss might result in major financial losses or serious injuries to personnel.
- **High**—Indicates a severe or catastrophic adverse effect. Note that *high* indicates one adverse effect. *Very high* indicates multiple adverse effects.
- **Moderate**—Indicates a serious adverse effect. *Serious* indicates critical business functions are significantly degraded. The organization might still be able to operate but not as effectively as normal. The resulting damage can be significant.
- **Low**—Indicates a limited adverse effect. *Limited* indicates critical business functions are degraded. The resulting damage is minor.
- **Very low**—Indicates a negligible adverse effect. *Negligible* indicates the impact on critical business functions is small and unnoticeable.

Classify Business Risks

The way in which individuals and businesses use their assets varies across all industries. If a person looks at risk and its impact to the organization, he or she could quickly become overwhelmed trying to create a comprehensive list of all the possible threats and vulnerabilities that affect the company. Luckily, there are several techniques that can help direct

this activity. The following method achieves this by focusing the task on the risks posed by the people, process, and technology of the organization.

Risks Posed by People

Ideally, all personnel in an organization should readily understand the threat to a company's health if risk is not managed. Unfortunately, risks and risk management are often perceived quite differently. Personnel often tend to be the weakest link when it comes to security threats to an organization.

One of the challenges with effective risk management of IT resources is achieving a proper balance between security and usability. **FIGURE 1-2** shows a diagram. In the diagram, on the left, the computers are completely locked down with such a high level of security that the controls may prevent users from adequately performing their jobs. On the right, the computers are easy to use, but security is being neglected. In the middle, a balance between the two has been achieved.

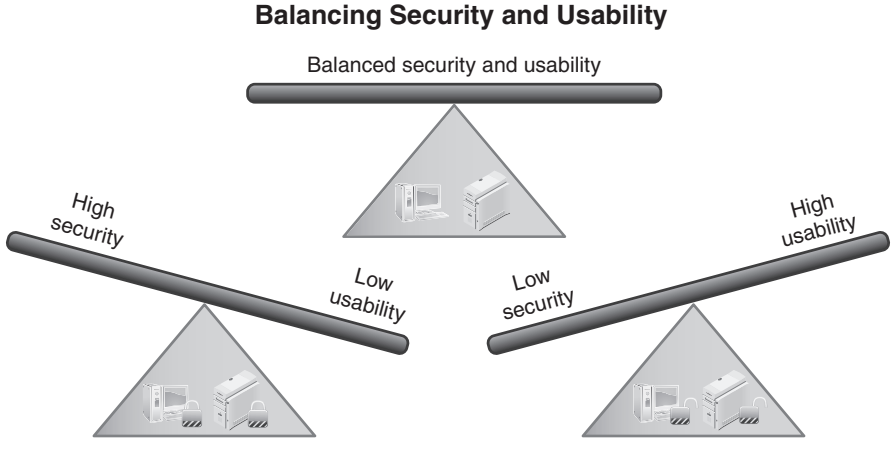
Balanced security rarely satisfies everyone. Security personnel want to lock systems down tight, whereas end users find those security controls inconvenient and want more usability.

It is common for individuals in the following roles to have different perceptions of risk:

- **Leaders and managers**—Leaders and managers are concerned mostly with profitability and survivability. Because attacks can result in loss of C-I-A, leaders are willing to spend money to mitigate risks. However, their view of risk is typically based on costs associated with the risk and the controls. Managers need accurate facts to make decisions regarding which controls to implement to protect company assets.
- **System administrators**—System administrators are responsible for protecting IT systems. When they understand the risks, they often want to lock systems down as tight as possible. Administrators are often highly technical individuals. Sometimes, they lose sight of the need to balance security costs with profitability. Some organizations have

FIGURE 1-2

Balancing security and usability in an organization.



administrators, often Tier 1, who serve as the first line of defense for IT support. These administrators are given limited administrative permissions. They often view the security controls as hindrances to performing their job and don't always recognize the importance of the controls. For example, the need to use a change management process isn't always understood. A well-meaning technician may bypass a change management process to solve one problem but unintentionally create another problem. These unapproved changes can result in business losses.

- **Developer**—Some companies have in-house application developers. They write applications that can be used in-house or sold as part of the company's product offerings. Many developers have adopted a secure computing mindset. They realize that security needs to be included beginning at the design stage and going all the way through to the release stage. When developers haven't adopted a security mindset, they often try to patch security holes at the end of the development cycle. This patching mindset rarely addresses all problems and results in the release of vulnerable software. Ideally, security needs to be an integral step in the life cycle of software or application development.
- **End user**—End users simply want the computer to work for them. They are most concerned with usability and often don't understand the reason for the security controls and restrictions. Instead, security is viewed as an inconvenience. Well-meaning users often try to circumvent controls so they can accomplish their job. For example, because USB thumb drives often transport viruses without the user's knowledge, companies frequently implement policies restricting the use of thumb drives. However, a user who needs to transfer a file from one computer to another to complete a project deadline may view a USB thumb drive as a necessary solution.

TIP

The use of thumb drives can be restricted through a written policy telling people not to use them as well as by using technical controls. Computer users can easily ignore a written policy, but they can't easily bypass a technical control. A best practice is to create and enforce both types of policies, written and technical.

The perceptions of these different role holders can be addressed through targeted training. Some training can include all employees. Other training should be targeted to specific roles. Targeted training helps role holders better understand the big picture. It can also help them understand the importance of security and its value to the success of the company. People responsible for managing risks must take all perceptions into account. This is especially true if any of the controls can be bypassed. For example, theft of laptops is a common problem for some companies. An employee can leave a laptop to take a break at a conference only to come back and find the laptop gone. This risk can almost be eliminated if the company purchases hardware locks, which can secure the laptop to a desk or other furniture. However, if users don't perceive the risk as valid, they may simply not use the lock; therefore, they must be trained to understand the controls and the consequences (to the company and themselves) for not complying with the controls.

Risks Posed by a Lack of Process

Process represents the actions taken to reach a desired outcome. A lack of formal process is a contributor to risk in any organization. Without a process for creating recipes and training cooks, a bakery, for example, could not produce consistently delicious cupcakes, and

risks income loss. Without a process for inventory control, a sales company may risk loss of customers from lack of supply. For many organizations, these processes take the form of policies, standards, and guidelines. The following list describes some of the processes associated with IT resources:

- **Policies—Policies** are formal statements that are issued directly by an organization's leaders, such as an acceptable use policy, which describes both acceptable and unacceptable behavior when using company-owned computers and network resources.
- **Standards—Standards** are mandatory rules written to support or at least provide some direction to policies. For example, a password standard could follow an acceptable use policy.
- **Guidelines—Guidelines** are not mandatory but provide guidance on specific behavior. For example, guidelines are written on how to create a strong password.

Ideally all organizations should have a general information security policy and may have specific policies in place to define how the business will handle access control, remote access, email usage, incident response, disaster recovery, business continuity, and other risk situations.

Risks Posed by Technology

Whether in a small business, large government body, or publicly traded corporation, most IT infrastructures consist of the seven domains shown in **FIGURE 1-3**: User, Workstation, LAN, LAN-to-WAN, WAN, Remote Access, and System/Application. Each domain poses its own set of risks. One method for identifying the risks posed by technology is to review each domain, concentrating on the threats, vulnerabilities, and impact of a loss.

The following examples describe *some* of the risks for each domain; more risks exist than are described for each domain. Businesses must provide protection in each of the domains. A weakness in any one of the domains can be exploited by an attacker even if the other six domains have no vulnerabilities.

User Domain

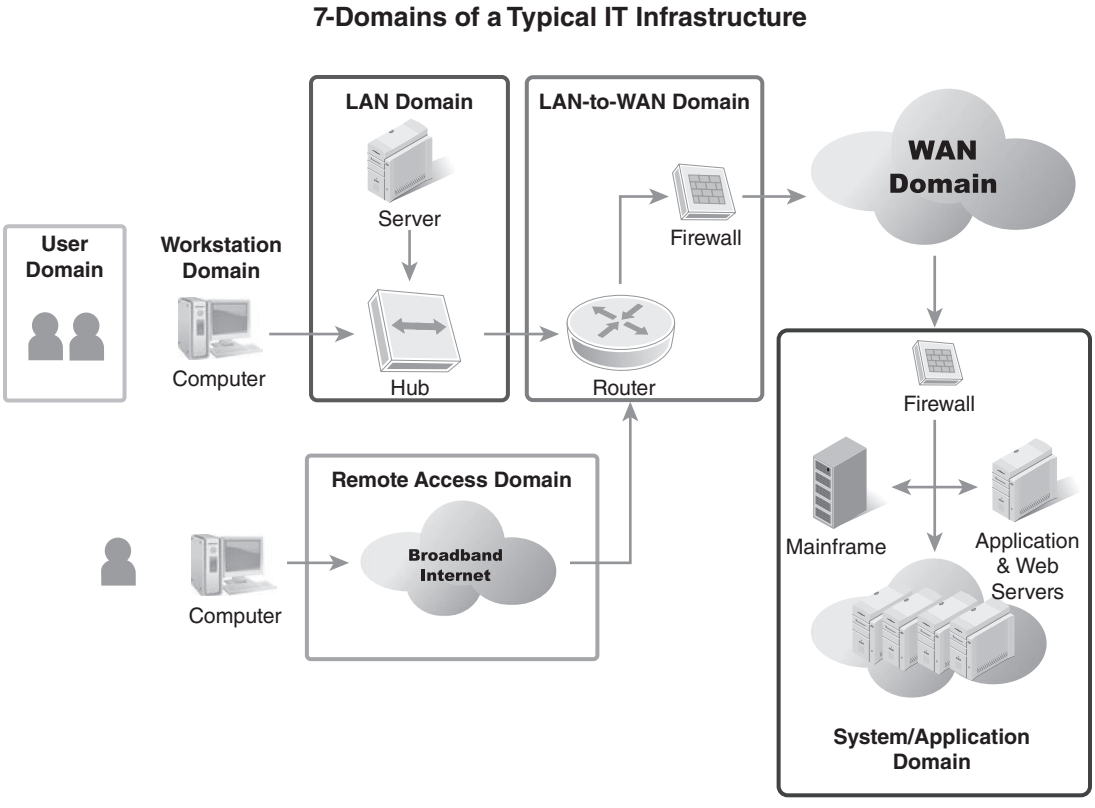
The User Domain defines the way in which people interact with an organization's information system. They can be customers, employees, contractors, or consultants. The old saying that a chain is only as strong as its weakest link applies to IT security too. People are often the weakest link in IT security. For example, an organization may require strong, complex passwords that can't be easily cracked, but an employee may write his or her password on a sticky note, leaving the organization vulnerable to unauthorized access.

Workstation Domain

A workstation can be a desktop or a laptop computer, a special-purpose terminal, or any other device that connects to an organization's network; a workstation is where users first access the systems, applications, and data of the organization. The Workstation Domain requires tight security and access controls. In addition, bugs and vulnerabilities are constantly being discovered in operating systems and applications. Software vendors regularly release patches and fixes that must be applied to help keep the systems protected.

FIGURE 1-3

The seven domains of a typical IT infrastructure.



LAN Domain

The LAN Domain is the area that is inside the firewall. A local area network (LAN) can be a single workstation and printer connected in a small home office network or a large network with thousands of devices. Because these devices share network resources, they are vulnerable to a threat that attacks a single device. For example, a user may visit risky websites and unknowingly download a virus that can infect the entire network.

LAN-to-WAN Domain

The LAN-to-WAN Domain is where the IT infrastructure links to a wide area network (WAN) and the Internet. The LAN-to-WAN Domain provides Internet access for the entire organization and acts as the entry and exit point for the WAN. The public side of the boundary is often connected to the Internet and is a frequent target of hackers looking for vulnerabilities that will allow unauthorized access to the LAN.

WAN Domain

The Wide Area Network (WAN) Domain connects remote locations. The goal of managing the WAN Domain is to allow users the most access possible while making sure that what goes in and out is safe. A significant amount of security is required to keep hosts

in the WAN Domain safe. Risks associated with this domain include eavesdropping and authorized access because most traffic in this domain is sent in cleartext, which means that hackers can access usernames and passwords. In addition, data is subject to corruption and malicious attacks.

NOTE

VPN connections use tunneling protocols to reduce the risk of data being captured. A tunneling protocol encrypts the traffic sent over the network, which makes it more difficult for attackers to capture and read data.

TIP

A server should be locked down using the specific security requirements needed by the hosted application. In other words, an email server requires one set of protections, which is different from that required for a database server.

Remote Access Domain

The Remote Access Domain connects remote users to the organization's IT infrastructure. Remote access is critical for staff members who work in the field or from home, for example, outside sales reps, technical support specialists, or health care professionals. Wi-Fi hotspots make it easy for users to connect to a virtual private network (VPN) to access email and other business applications, but it also poses risks to the organization's proprietary data if the employee's device is stolen or left unsecured.

System/Application Domain

The System/Application Domain is where the organization's data is stored. This data can be private customer data, intellectual property, or national security information. Data is what attackers seek deep within an IT system. Loss of this data, whether by attack, disaster, or negligence, is the greatest threat in the System/Application Domain.

Risk Identification Techniques

Risk and losses were presented earlier in this chapter. Risk is the likelihood or probability that something unexpected is going to occur. Some risks lead to losses. Losses occur when a threat exposes a vulnerability and harms an asset. To identify risks, these three steps need to be followed:

1. Identifying threats
2. Identifying vulnerabilities
3. Estimating the likelihood of a threat exploiting a vulnerability to harm an asset

The following sections explore these concepts.

Identifying Threats

A threat is any circumstance or event with the potential to cause a loss. Said another way, it is any activity that represents a possible danger. The loss or danger is directly related to one of the following:

- **Loss of confidentiality**—Someone sees a person's password or a company's "secret formula."
- **Loss of integrity**—An email message is modified in transit, a virus infects a file, or someone makes unauthorized changes to a website.

- **Loss of availability**—An email server is down so no one has email access, or a file server is down so data files aren't available.

Threat identification is the process of creating a list of threats. Companies should attempt to identify *all* possible threats to an organization, which is no small task. The list can be extensive.

To compile this list of threats, businesses often consider threats in the following categories:

- **External or internal**—External threats are outside the boundary of the organization. They can also be thought of as risks that are outside the control of the organization. Internal threats are within the boundary of the organization. They could be related to employees or other personnel who have access to company resources. Internal threats can be related to any hardware or software controlled by the business.
- **Natural or man-made**—Natural threats are often related to weather, such as hurricanes, tornadoes, and ice storms. Earthquakes and tsunamis are also natural threats. A human, or man-made, threat is any threat from a person. Any attempt to sabotage resources is a man-made threat. Fire could be man-made or natural, depending on how the fire is started.
- **Intentional or accidental**—Any deliberate attempt to compromise confidentiality, integrity, or availability is intentional. Employee mistakes or user errors are accidental threats. A faulty application that corrupts data could be considered accidental.

One method used to identify threats is through a brainstorming session. In a brainstorming session, participants throw out anything that pops into their heads. All ideas are written down without any evaluation. This creative process helps bring up ideas that may be missed when a problem is analyzed only logically.

Examples of threats to an organization include:

- An unauthorized employee trying to access data
- Any type of malware
- An attacker defacing a website
- Any DoS or DDoS attack
- An external attacker trying to access data
- Any loss of data
- Any loss of services
- A social engineer tricking an employee into revealing a secret
- Earthquakes, floods, or hurricanes
- A lightning strike
- Electrical, heating, or air-conditioning outages
- Fires

All these threats represent possible risks if they expose vulnerabilities and potentially harm assets.

Of course, threats and vulnerabilities will be identified that are particular to an organization. In fact, a business with multiple locations may have some threats and vulnerabilities unique to each location.

Identifying Vulnerabilities

That a vulnerability is a weakness was presented earlier in the chapter. Vulnerabilities become apparent when threats exploit them. Ideally, the weaknesses would be identified before threats exploit them. Luckily, most organizations have many sources that can help a person do this.

Some of the sources that can be used are:

- **Audits**—Many organizations are regularly audited. Systems and processes are checked to verify that a company complies with existing rules and laws. Auditors document their findings in reports, which list findings that directly relate to weaknesses.
- **Certification and accreditation records**—Several standards exist to examine and certify IT systems. If the system meets the standards, the IT system can be accredited. The entire process includes detailed documentation. This documentation can be reviewed to identify existing and potential weaknesses.
- **System logs**—Many types of computer system logs can be used to identify threats. Audit logs can determine whether users are accessing sensitive data. Firewall logs can identify traffic that is trying to breach the network and computers taken over by malware and acting as zombies. Domain Name System (DNS) logs can identify unauthorized transfer of data.
- **Prior events**—Previous security incidents are excellent sources of data. As evidence of risks that already occurred, they help justify controls. They show the problems that have occurred and can show trends. Ideally, weaknesses from a security incident will be resolved right after the incident. In practice, sometimes, employees are eager to put the incident behind them and forget it as soon as possible. Even if documentation doesn't exist on the incident, a few key questions can uncover the details.
- **Trouble reports**—Most companies use databases to document trouble calls. These databases can contain a wealth of information. With a little analysis, they can be used to identify trends and weaknesses.
- I**ncident response teams**—Some companies have incident response teams. These teams will investigate all the security incidents within the company. Team members can be interviewed to get a wealth of information because they are often eager to help reduce risks.

Using the Seven Domains of a Typical IT Infrastructure to Identify Weaknesses

Another way of identifying weaknesses is by examining the seven domains of a typical IT infrastructure, which were presented earlier in this chapter. Each domain can be examined individually. Further, each domain can be examined by experts in that domain. The following list provides examples of vulnerabilities in each of these domains:

- **User Domain**—Social engineering represents a big vulnerability. For example, Sally gets a call: "Hi, this is Bob from the help desk. We've identified a virus on your computer." Bob then attempts to walk Sally through a long, detailed process and then says, "Why don't I just fix this for you so you can get back to work? All I need is your password."

- **Workstation Domain**—Computers that aren't patched can be exploited. If they don't have antivirus software, they can become infected.
- **LAN Domain**—Any data on the network that is not secured with appropriate access controls is vulnerable. Weak passwords can be cracked. Permissions that aren't assigned properly allow unauthorized access.
- **LAN-to-WAN Domain**—If users are allowed to visit malicious websites, they can mistakenly download malicious software. Firewalls with unnecessary ports open allow access to the internal network from the Internet.
- **WAN Domain**—Any public-facing server is susceptible to DoS and DDoS attacks. A File Transfer Protocol (FTP) server that allows anonymous uploads can host warez from black-hat hackers.
- **Remote Access Domain**—Remote users may be infected with a virus but not know it. When they connect to the internal network via remote access, the virus can infect the network.
- **System/Application Domain**—Database servers can be subject to SQL injection attacks. In an SQL injection attack, the attacker can read the entire database. SQL injection attacks can also modify data in the database.

This section does not represent a complete list; it couldn't. The number of vulnerabilities discovered in IT systems is constantly growing. The MITRE Corporation catalog **Common Vulnerabilities and Exposures (CVE)** currently includes more than 40,000 items.

TIP

Some malware can take control of multiple computers and control them as robots. The controlling computer issues attack commands, and the computers attack. The individual computers are referred to as *zombies*. The network of controlled computers is called a *botnet*.

TIP

Warez (pronounced "wares") is a term that describes pirated files. Examples include pirated games, MP3 files, and movies. A warez site often includes hacking tools, which anyone can download, including hackers.

TIP

An *SQL injection attack* tries to access data from websites. SQL statements are entered into text boxes. If the website isn't programmed defensively, these SQL statements can be executed against a database. Programs are available that can launch an SQL injection attack and retrieve an entire database.

Assessing Impact and Likelihood

The third step when identifying risks is to estimate the likelihood of a threat exploiting a vulnerability to harm an asset. Threats are matched to existing vulnerabilities to determine the impact of the threat to the organization.

Several threats are listed under the earlier section Identifying Threats. **TABLE 1-1** takes a few of those threats and matches them to vulnerabilities to identify the impact of possible losses.

The following formula is often used when pairing threats with vulnerabilities:

$$\text{Risk} = \text{Threat} \times \text{Vulnerability}$$

However, this isn't a true mathematical formula. Threat and vulnerability don't always have numerical values. Instead, the formula shows the relationship between the two.

If the value of the asset can be identified, the formula is slightly modified to:

$$\text{Total risk} = \text{Threat} \times \text{Vulnerability} \times \text{Asset value}$$

TABLE 1-1 Assessing the impact of a threat

THREAT	VULNERABILITY	IMPACT
An unauthorized employee tries to access data hosted on a server.	The organization doesn't use adequate authentication and access controls.	The possible loss would depend on the sensitivity of the data and how it's used. For example, if the unauthorized employee accessed salary data and freely shared it, morale and productivity could be impacted.
Any type of malware, such as viruses or worms, enters the network.	Antivirus software doesn't detect the virus.	The virus could be installed on systems. Viruses typically result in loss of confidentiality, integrity, or availability.
An attacker modifies or defaces a website.	The website isn't protected.	Depending on how the attacker modifies the website, the credibility of the company could be affected.
A social engineer tricks an employee into revealing a password.	Users aren't adequately trained.	Passwords could be revealed. An attacker who obtains a password could take control of the user's account.

Balancing Risk and Cost

The costs to manage the risk must be balanced against the impact value. The costs can be measured in actual monetary values if they are available. The costs can also be balanced by using relative values, such as *low, medium*, and *high*.

TABLE 1-2 shows an example of how the relative values can be assigned. Likelihood values are shown vertically, and impact values are shown horizontally. If a threat has a 0 to 10 percent likelihood of occurring, it is assigned a value of low. If the value is between 11 and 50 percent, the value is medium. If the value is between 51 and 100, the value is high. Similarly, the impact can be ranked as low, medium, and high.

Sometimes, the potential for risks to occur and their impact are very high, which presents an easy choice. For example, systems without antivirus software will become infected. The threat is common. The likelihood is high. If or when it happens, an infected system can result in the compromise or destruction of all the business's data. The impact is also high. This risk needs to be mitigated. The cost of antivirus software is far less than the impact costs. Therefore, antivirus software is commonly used in business.

Other times, the likelihood is low, but the impact is high. For example, the risk of fire in a data center is low. However, the impact is high. A business will often have fire detection and suppression equipment to prevent the impact should a fire occur. Insurance is also purchased to reduce the impact if a fire does cause damage.

Reasonableness

With so many risks threatening a company's business, realizing that the company doesn't need to manage every possible risk should be good news. Some risks are reasonable to manage, whereas others are not.

TABLE 1-2 A threat-likelihood–impact matrix

	LOW IMPACT (0%–10%)	MEDIUM IMPACT (11%–50%)	HIGH IMPACT (51%–100%)
High-threat likelihood—100% (1.0)	10 × 1 = 10	50 × 1 = 50	100 × 1 = 100
Medium-threat likelihood—50% (.50)	10 × .50 = 5	50 × .50 = 25	100 × .50 = 50
Low-threat likelihood—10% (.10)	10 × .10 = 1	50 × .10 = 5	100 × .10 = 10

Reasonableness is a test that can be applied to risk management to determine whether the risk should be managed. The test is derived from the reasonable-person standard in law. In short, this question should be answered: "Would a reasonable person be expected to manage this risk?"

Risks that don't meet the reasonableness test are accepted. For example, the threat of nuclear war exists. A company could spend resources on building bomb shelters for all employees and stocking them with food and water to last 30 years. However, this scenario just isn't reasonable.

As another example, consider a company located on the east coast of Florida. Hurricanes are a very real threat and should be considered. However, the likelihood of a major earthquake hitting the east coast of Florida is relatively minor and doesn't need to be addressed. A business in San Francisco, however, has different concerns. An earthquake there is a real threat but not a hurricane. So, for San Francisco, the risk of a hurricane is readily accepted, whereas the risk of an earthquake is not.

TIP

A more detailed threat-likelihood–impact matrix can be created. For example, instead of assigning values of low, medium, or high for the threat likelihood, actual percentages can be assigned. Also, more categories can be used, instead of just three. Using more categories allows greater separation between them. Similarly, any number within a range can be assigned to the impact. The matrix in Table 1-2 uses a range of 10, 50, and 100, but any numbers between 1 and 100 could be used.

Another standard of reasonableness is to focus on the vulnerabilities only within the organization or the system being evaluated. External vulnerabilities are often not addressed. For example, a server will likely fail if the air-conditioning fails. This situation would be addressed when vulnerabilities for a server room were being identified. This vulnerability wouldn't be addressed for each of the 50 servers in the server room. Similarly, the commercial power may fail. This situation may be addressed by having uninterruptible power supplies (UPSs) and generators. However, alternatives don't need to be identified for the commercial power company.

Risk Management Process

Earlier in this chapter, risk management was defined as the practice of identifying, assessing, controlling, and mitigating risks. Identifying the threats and vulnerabilities that are relevant to the organization is an important step, just as knowing the worth of an asset can help

determine the impact of its loss. With this information, action can then be taken to reduce potential losses to assets from these risks.

Realizing that risk management is not the same as risk elimination is important. Risk elimination isn't a reasonable goal. Instead, risk management attempts to identify the risks that can be minimized at a reasonable cost and implements controls to do so. Risk management includes several elements:

TIP

Risk management **controls** are any actions or changes put into place to reduce a weakness or potential loss. NIST Special Publication 800-37 Rev. 2 identifies three classes of controls: technical, administrative, and physical. More will be learned about controls later in this text.

TIP

Controls are often referred to as either preventive or detective. **Preventive controls** attempt to prevent the risk from occurring. Examples include increasing physical security and training personnel. **Detective controls** try to detect activity that may result in a loss. Examples include antivirus software and intrusion detection systems

- **Assessing risks**—Risk management starts with a **risk assessment**, or risk analysis. There are several steps to developing a risk assessment:
  - **Identifying the assets of an organization and their value**—When focused on IT, these assets can include data, hardware, software, services, and the components of the IT infrastructure itself.
  - **Identifying threats and vulnerabilities to the assets**—Prioritize the threats and vulnerabilities.
  - **Identifying the likelihood of a vulnerability being exploited by a threat**—These vulnerabilities are the risks.
  - **Identifying the impact of a risk**—Risks with higher impacts should be addressed first.
- **Identifying a risk response**—Risks can be avoided, shared or transferred, mitigated, or accepted. That decision is often based on the likelihood of the risk's occurring, the impact it would have if it does occur, and the cost to implement a sufficient control.
- **Selecting controls**—After the risks have been identified, control methods can be identified and selected. Control methods are also referred to as *countermeasures*. Controls are primarily focused on reducing vulnerabilities and impacts.
- **Implementing and testing controls**—Once the controls have been implemented, they can be tested to ensure they provide the expected protection.
- **Evaluating controls**—Risk management is an ongoing process. Implemented controls should regularly be evaluated to determine whether they still provide the expected protection. Evaluation is often done by performing regular vulnerability assessments.

Cost-Benefit Analysis

After risks have been identified, steps can be taken to reduce or manage them, often by implementing controls, or countermeasures. Managing risks comes at a cost. If too much money is spent on reducing risks, the business's overall profit will be reduced. If too little money is spent on reducing risks, a loss could result from an easily avoidable threat and/or vulnerability. Ideally, organizations should never spend more on controls than the value of the asset. For example, an organization should not spend $10,000 in controls for an asset that is worth only $5,000. The amount spent on controls should be proportional to the risk, which is known as the **principle of proportionality**.

Risks can be measured based on the value of the asset. A **cost-benefit analysis (CBA)** can be performed to help determine which controls, or countermeasures, to implement. If the benefits outweigh the costs, the control is often selected.

A CBA compares the business impact with the cost to implement a control. For example, the loss of data on a file server may represent the loss of $1 million worth of research. Implementing a backup plan to ensure the availability of the data may cost $10,000. In other words, $10,000 would be spent to save $1 million, which makes sense.

Starting a CBA begins by gathering data to identify the costs of the controls and benefits gained if they are implemented.

- **Cost of the control**—Cost of the control includes the purchase costs plus the operational costs over the lifetime of the control.
- **Projected benefits**—Projected benefits include the potential benefits gained from implementing the control. These benefits are identified by examining the costs of the loss and how much the loss would be reduced if the control were implemented.

A control doesn't always eliminate the loss. Instead, the control reduces it. For example, annual losses for a current risk may average $100,000. If a control is implemented, these losses may be reduced to $10,000. Thus, the benefit of the control is $90,000.

The following formula can be used to determine whether the control should be used:

Loss before control – Loss after control = Cost of control

For example, the company lost $100,000 last year without any controls implemented. If the control is implemented, a loss of $12,000 a year is estimated. The cost of the control is estimated at $7,000. The formula is:

$100,000 – $7,000 (Cost of control) – $12,000 (Expected residual loss) = $81,000

Implementing the control represents a benefit of $81,000.

One of the biggest challenges when performing a CBA is getting accurate data. Although current losses are often easily available, future costs and benefits need to be estimated. Costs are often underestimated, and benefits are often overestimated.

The immediate costs of a control are often available. However, sometimes, the ongoing costs are hidden. Some of the hidden costs may be:

- Costs to train employees
- Costs for ongoing maintenance
- Software and hardware renewal costs, such as subscription costs

Following the principle of proportionality, if the costs outweigh the benefits, the organization might choose not to implement the control. Instead, it might choose to accept, share or transfer, or avoid the risk.

Profitability Versus Survivability

Both **profitability** and **survivability** must be considered when evaluating the cost of risk management:

- **Profitability**—Profitability is the ability of a company to make a profit. It is calculated as revenues minus costs.
- **Survivability**—Survivability is the ability of a company to survive a loss due to a risk. Some losses, such as fire, can be disastrous and will cause the business to fail.

In terms of profitability, a loss can ruin a business. In terms of survivability, a loss may cause a company never to earn a profit. The costs associated with risk management don't contribute directly to revenue gains. Instead, these costs help to ensure that a company can continue to operate even if it incurs a loss.

Regarding profitability and survivability, the following items should be considered:

- **Out-of-pocket costs**—The cost to reduce risks comes from existing funds.
- **Lost opportunity costs**—Money spent to reduce risks can't be spent elsewhere, which may result in lost opportunities if the money could be used for other purposes.
- **Future costs**—Some countermeasures require ongoing or future costs. These costs could be for renewing hardware or software. Future costs can also include the cost of employees to implement the countermeasures.
- **Client and stakeholder confidence**—The value of client and stakeholder confidence is also important. If risks aren't addressed, clients and stakeholders may lose confidence when a threat exploits a vulnerability, resulting in a significant loss to the company.
- **Total cost of security**—The total cost of security includes one-time costs, for example, spending money on an IDS, and ongoing, or recurring, costs, for example, the cost of an antivirus software subscription. This cost can be quite high, and the money spent reduces the company's overall profit. But what's the alternative? If these protections are not taken, the entire business could grind to a halt. If this happens too often or for too long, the business could fail.

Data is often one of the most valuable assets a business owns. It can include customer data; accounting data, such as accounts payable and accounts receivable; and employee data. The list could go on and on. This data is integral to the success of a business, so it is often backed up regularly.

For example, a business spends $15,000 a year on data backups, a cost that will not increase revenue or profits. In a full year's time, data is never lost, and the backups are never needed. If profitability is the only consideration, management may decide to eliminate this cost. Backups are stopped, but the next year, data could be lost, causing the company to fail and go bankrupt.

The cost does need to be considered against profitability, though. For example, if a company earns only $10,000 a year in profit, the company's spending $15,000 a year to protect its data doesn't make sense.

On the other hand, for example, a company has $100,000 in annual profits. It chooses not to spend the $15,000 on backups, but then a virus spreads through the enterprise, destroying all customer and accounting data. The company no longer has reliable records of accounts receivable, and no one has access to the customer base. Such a scenario can be a business-ending catastrophe.

Risk-Handling Strategies

Risk management can also be thought of as handling risk. Remembering that risk management is not risk elimination is important. A business that is unwilling to take any risks doesn't stay in business for long because the cost to eliminate all risks would consume all the profits.

The ultimate goal of risk management is to protect the organization. It helps ensure a business can continue to operate and earn a profit. Risk management includes several steps:

- Identifying risks
- Assessing risks
- Determining which risks will be handled and which risks will be accepted
- Taking steps to reduce risks to an acceptable level

A risk can be avoided, shared or transferred, mitigated, or accepted. Each of these techniques is explained in the following sections.

Avoiding

One of the ways risks can be managed is by simply avoiding them. The primary reason for **avoiding** a risk is when the impact of the risk outweighs the benefit of the asset.

An organization can avoid risk by:

- **Eliminating the source of the risk**—The company can stop the risky activity. For example, a company may have a wireless network that is vulnerable to attacks. The risk could be avoided by removing the wireless network, which can be done if the wireless network isn't an important asset in the company.
- **Eliminating the exposure of assets to the risk**—The company can move the asset. For example, a data center could be at risk because it is located where earthquakes are common. It could be moved to an earthquake-free zone to eliminate this risk, but the cost to move the data center would be high. However, if the risk is unacceptable and the value of the data center is high, it makes sense.

Sharing or Transferring

Sharing or **transferring** risk means shifting responsibility to another party. Transferring risk shifts the entire responsibility or liability. Sharing risk shifts a portion of the responsibility or liability. Organizations can outsource part or all of the activity.

- **Insurance**—A company can purchase insurance to protect it from a loss. If a loss occurs, the insurance covers it. Many types of insurance are available, including fire insurance.
- **Outsourcing the activity**—For example, a company may want to host a website on the Internet. The company can host the website with a web-hosting provider. The company and the provider can agree on who assumes responsibility for security, backups, and availability.

Mitigating

Risk is reduced by reducing vulnerabilities. The primary strategy in this process is **mitigating** risks. Mitigating risks is also known as *risk reduction*.

Implementing controls, or countermeasures, reduces vulnerabilities. The cost of a control should not exceed the benefit. Determining costs and benefits often requires a CBA, which was covered earlier in this chapter.

Examples of mitigation steps are:

- **Alter the physical environment**—Replace hubs with switches. Locate servers in locked server rooms.
- **Change procedures**—Implement a backup plan. Store a copy of backups off-site, and test the backups.
- **Add fault tolerance**—Use RAIDs for important data stored on disks. Use failover clusters to protect servers.
- **Modify the technical environment**—Increase security on the firewalls. Add IDSs. Keep antivirus software up to date.
- **Train employees**—Train technical personnel on how to implement controls. Train end users on social engineering tactics.

Often, the goal is not to eliminate the risk but, instead, to make it too expensive for the attacker. Here are two formulas:

- **Attacker's cost < Attacker's gain**—When this is true, attacking is appealing to the attacker.
- **Attacker's cost > Attacker's gain**—When this is true, the attacker is less likely to pursue the attack.

Cryptography is one of the ways to increase the attacker's cost. If a company sends data across the network in cleartext, the data can be captured and analyzed. If the company encrypts the data, an attacker must decrypt it before analyzing it. The goal of the encryption isn't to make it impossible to decrypt the data. Instead, the goal is to make it too expensive or time consuming for the attacker to crack it.

NOTE

A simple failover cluster could include two servers. One server provides the service to users, and the other server acts as a spare. If the online server fails, the spare server can sense the failure and automatically take over.

Accepting

Accepting a risk is another choice. A company can evaluate a risk, understand the potential loss, and choose to accept it, which is commonly done when the cost of the control outweighs the potential loss.

For example, a company hosts a web server used for e-commerce. The web server generates about $1,000 per month in revenue. The server could be protected using a failover cluster. However, estimates indicate that a failover cluster will cost approximately $10,000. If the server goes down, it may be down for only one or two hours, which equates to less than $3 (Revenue per hour = $1,000 × 12 / 365 / 24 = $1.37).

Residual Risk

Residual risk is the risk that remains after controls have been applied. Eliminating all risks is not feasible. Instead, steps are taken to reduce the risk to an acceptable level. The risk that's left is residual risk.

Earlier in this chapter, the following two formulas were given for risk:

$$\text{Risk} = \text{Threat} \times \text{Vulnerability}$$

$$\text{Total risk} = \text{Threat} \times \text{Vulnerability} \times \text{Asset value}$$

The following formula can be used to calculate residual risk:

$$\text{Residual risk} = \text{Total risk} - \text{Controls}$$

Senior managers are responsible for losses due to residual risk. They decide whether a risk should be avoided, shared or transferred, mitigated, or accepted. They also decide which controls to implement. Any resulting loss due to their decisions falls on their shoulders.

CHAPTER SUMMARY

Risks occur when threats exploit vulnerabilities and result in a loss. The loss can compromise assets and core business functions. The impact of losses can be seen in business costs. The steps in risk management are to identify threats and vulnerabilities, which can then be paired to help determine the impact of the risk. By implementing controls, vulnerabilities can be reduced. The amount spent on controls should be proportional to the risk.

By choosing one of four techniques, avoiding, sharing or transferring, mitigating, or accepting, risks can be managed. The primary risk management technique is mitigating risk, which is also known as risk reduction or risk treatment. Deciding to accept a loss becomes easier if a CBA has been completed.

KEY CONCEPTS AND TERMS

accepting
asset
availability
avoiding
audit
business function
Common Vulnerabilities and Exposures (CVE)
confidentiality
control
cost-benefit analysis (CBA)
denial of service (DDoS) attack
detective control
disaster recovery
distributed denial of service (DDoS) attack
exploit
goodwill
guideline
impact of loss
intangible value
integrity
mitigating
policy
preventive control
principle of proportionality
profitability
reasonableness
residual risk
risk
risk assessment
risk management
sharing
social engineering
standard
survivability
tangible value
threat
transferring
vulnerability

CHAPTER 1 ASSESSMENT

1. Which one of the following properly defines risk?

A. Threat × Mitigation
B. Vulnerability × Controls
C. Controls – Residual risk
D. Threat × Vulnerability

2. Which one of the following properly defines total risk?

A. Threat – Mitigation
B. Threat × Vulnerability × Asset value
C. Vulnerability – Controls
D. Vulnerability × Controls

3. The best bet is to reduce risk to a level that can be accepted.

A. True
B. False

4. Which of the following are accurate pairings of threat categories? (Select two.)

A. External and internal
B. Natural and supernatural
C. Intentional and accidental
D. Computer and user

5. A loss of client confidence or public trust is an example of a loss of _____.

6. A _____ is used to reduce a vulnerability.

7. As long as a company is profitable, it does not need to consider survivability.

A. True
B. False

8. What is the primary goal of an information security program?

A. To eliminate losses related to employee actions
B. To eliminate losses related to risk
C. To reduce losses related to residual risk
D. To reduce losses related to loss of confidentiality, integrity, and availability

9. The _____ is an industry-recognized standard list of common vulnerabilities.

10. Which of the following is a goal of risk management?

A. To identify the correct cost balance between risk and controls
B. To eliminate risk by implementing controls
C. To eliminate the loss associated with risk
D. To calculate value associated with residual risk

11. If the benefits outweigh the cost, a control is implemented. Costs and benefits are identified by completing a _____.

12. A company decides to reduce losses of a threat by purchasing insurance, which is known as risk _____.

13. What can be done to manage risk? (Select three.)

A. Accept it
B. Transfer it
C. Avoid it
D. Migrate it

14. After controls to minimize risk in the environment have been applied, what is the remaining risk called?

A. Remaining risk
B. Mitigated risk
C. Managed risk
D. Residual risk

15. Who is ultimately responsible for losses resulting from residual risk?

A. End users
B. Technical staff
C. Senior managers
D. Security personnel

CHAPTER 2

Managing Risk: Threats, Vulnerabilities, and Exploits

ORGANIZATIONAL ASSETS include data, people, process, and technology systems. These assets face real threats every day and sometimes are unavoidable. To manage the risks that these threats pose, which assets need to be protected and the source of these threats must be identified. Additionally, what vulnerabilities are present in the assets that could be exploited by the threats is important to know. Threats usually exploit vulnerabilities to harm an asset. An understanding of the relationship between threat and vulnerability (also known as the threat/vulnerability pair) is important to mitigate risks.

The U.S. federal government has done much in the information security space, including developing frameworks to help understand and manage risks regarding organizational assets. One example of a framework is the Risk Management Framework (RMF) from the National Institute of Standards and Technology (NIST). The NIST RMF 800 special publications series provides a set of policies and standards that cover the life cycle of risk activities. These publications are freely available on the NIST.gov website. Additionally, the Department of Homeland Security (DHS) oversees several other initiatives related to information technology (IT) security.

Chapter 2 Topics

This chapter covers the following topics and concepts:

- What assets are and why they need to be managed
- What threats are and how they can be managed
- What vulnerabilities are and how they can be managed
- What exploits are and how they can be managed
- What the value of the risk management initiatives that the U.S. federal government sponsors is

Chapter 2 Goals

When you complete this chapter, you will be able to:

- Explain what assets are and why they need to be protected
- Describe the uncontrollable nature of threats
- List unintentional and intentional threats

- Identify best practices for managing threats
- Identify threat/vulnerability pairs
- Define *mitigation*
- List and describe methods used to mitigate vulnerabilities
- Identify best practices for managing vulnerabilities
- Define *exploit*
- Describe the perpetrator's role in vulnerabilities and exploits
- Identify mitigation techniques
- Identify best practices for managing exploits
- Identify the purpose of U.S. federal government risk management initiatives

Understanding and Protecting Assets

An asset represents anything of value that needs to be protected. In the IT world, assets include data, people, processes, and technology systems. The people who run technology systems and the processes that the organization has developed, such as policies, standards, and guidelines, are important assets worth protecting, just like the data in the technology systems is. Weaknesses in any of these areas can be exploited by threats to harm these assets. Organizations need to protect their assets; otherwise, the businesses become far more difficult to manage or even cease to exist.

Understanding and Managing Threats

A threat is any actor or activity that represents a possible danger to an asset. Threats include any circumstances or events with the potential to adversely impact confidentiality, integrity, or availability of a business's assets.

Threats are a part of the equation that creates risk:

$$\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Asset}$$

$$R = TVA$$

Any attempt to manage risk requires a thorough knowledge of threats. This section includes the following topics:

- Uncontrollable nature of threats
- Unintentional threats