

PART ONE

Risk Management Business Challenges

CHAPTER 1 Risk Management Fundamentals 2

CHAPTER 2 Managing Risk: Threats,
Vulnerabilities, and Exploits 29

CHAPTER 3 Managing Compliance 57

CHAPTER 4 Developing a Risk Management Plan 85

Risk Management Fundamentals

RISK MANAGEMENT IS IMPORTANT to the success of every company—a company that takes no risks doesn't thrive. On the other hand, a company that ignores risk can fail when a single threat is exploited. Nowadays, information technology (IT) systems contribute to the success of most companies. If you don't properly manage IT risks, they can also contribute to your company's failure.

Effective risk management starts by understanding threats and vulnerabilities. You build on this knowledge by identifying ways to mitigate the risks. Risks can be mitigated by reducing vulnerabilities or reducing the impact of the risk. You can then create different plans to mitigate risks in different areas of the company. A company typically has several risk mitigation plans in place.

Risk management is presented in three parts in this textbook. Part 1 is titled "Risk Management Business Challenges." It lays a foundation for the book, with definitions of many of the terms and techniques of risk management. It finishes with details on how to develop a risk management plan. Part 2 is titled "Mitigating Risk." This section covers risk assessments. Once you identify risks, you can take steps to reduce them. It ends with methods for turning a risk assessment into a risk mitigation plan. Part 3 is titled "Risk Management Plans." Here you learn how to create and implement several different plans, such as the business continuity plan and the disaster recovery plan.

This book can help you build a solid foundation in risk management as it relates to information system security. It won't make you an expert. Many of the topics presented in a few paragraphs in this book can fill entire chapters or even entire books. You'll find a list of resources at the end of the book. Use these resources to dig deeper into the topics that interest you. The more you learn, the closer you'll be to becoming the expert that others seek to solve their problems.

Chapter 1 Topics

This chapter covers the following topics and concepts:

- What risk is and what its relationship to threat, vulnerability, and loss is
- What the major components of risk to an IT infrastructure are
- What risk management is and how it is important 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 between threats and vulnerabilities, and impact
- 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

NOTE

The *Official (ISC)² Guide to the SSCP CBK* provides a more technical definition of risk. Risk is “the probability that a particular security threat will exploit a particular vulnerability.” If you’re not familiar with the alphabet soup, the (ISC)² System Security Certified Practitioner (SSCP) certification includes seven domains that are derived from a common body of knowledge (CBK).

NOTE

Threats and vulnerabilities are explored in much more depth later in this chapter, and later in this book.

What Is Risk?

Risk is the likelihood that a loss will occur. Losses occur when a **threat** exposes a **vulnerability**. Organizations of all sizes face risks. Some risks are so severe they cause a business to fail. Other risks are minor and can be accepted without another thought. Companies use risk management techniques to identify and differentiate severe risks from minor risks. When this is done properly, administrators and managers can intelligently decide what to do about any type of risk. The end result is a decision to avoid, transfer, mitigate, or accept a risk.

The common themes of these definitions are threat, vulnerability, and loss. Even though the common body of knowledge (CBK)—see note—doesn’t specifically mention loss, it implies it. Here’s a short definition of each of these terms:

- **Threat**—A threat is any activity that represents a possible danger.
- **Vulnerability**—A vulnerability is a weakness.
- **Loss**—A loss results in a compromise to business functions or assets.

Risks to a business can result in a loss that negatively affects the business. A business commonly tries to limit its exposure to risks. The overall goal is to reduce the losses that can occur from risk. Business losses can be thought of in the following terms:

- Compromise of business functions
- Compromise of business assets
- Driver of business costs

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 much. 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 e-mail customers. If the capabilities of either phones or e-mail are reduced, sales are reduced.
- A Web site sells products on the Internet. If the Web site is attacked and fails, sales are lost.
- Authors write articles that must be submitted by a deadline to be published. If the author’s PC becomes infected with a virus, the deadline passes and the article’s value is reduced.

CHAPTER 1 | Risk Management Fundamentals

- 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 they are located. If the application fails, products aren't shipped on time.

Because compromises to any of these business functions can result in a loss of revenue, they all represent risks. One of the tasks when considering risk is identifying the important functions for a business.

The importance of any business function is relative to the business. In other words, the failure of a Web site for one company may be catastrophic if all products and services are sold through the Web site. Another company may host a Web site to provide information to potential customers. If it fails, it will have less impact on the business.

Compromise of Business Assets

A business asset is anything that has measurable value to a company. If an asset has the potential of losing value, it is at risk. Value is defined as the worth of an asset to a business. Value can often be expressed in monetary terms, such as \$5,000.

Assets can have both tangible and intangible values. The **tangible value** is the actual cost of the asset. The **intangible value** is value that cannot be measured by cost, such as client confidence. Generally acceptable accounting principles (GAAP) refer to client confidence as goodwill.

Imagine that your company sells products via a Web site. The Web site earns \$5,000 an hour in revenue. Now, imagine that the Web server hosting the Web site fails and is down for two hours. The costs to repair it total \$1,000. What is the tangible loss?

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

The intangible value isn't as easy to calculate but is still very important. Imagine that several customers tried to make a purchase when the Web site was down. If the same product is available somewhere else, they probably bought the product elsewhere. That lost revenue is the tangible value.

However, if the experience is positive with the other business, where will the customers go the next time they want to purchase this product? It's very possible the other business has just gained new customers and you have lost some. The intangible value includes:

- **Future lost revenue**—Any additional purchases the customers make with the other company is a loss to your company.
- **Cost of gaining the customer**—A lot of money is invested to attract customers. It is much easier to sell to a repeat customer than it is to acquire a new customer. If you lose a customer, you lose the investment.

- **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.

Some examples of tangible assets are:

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

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

Driver of Business Costs

Risk is also a driver of business costs. Once risks are identified, steps can be taken to reduce or manage the risk. Risks are often managed by implementing countermeasures or controls. The costs of managing risk need to be considered in total business costs.

If too much money is spent on reducing risk, the overall profit is reduced. If too little money is spent on these controls, a loss could result from an easily avoidable threat and/or vulnerability.

Profitability Versus Survivability

Both **profitability** and **survivability** must be considered when considering risks.

- **Profitability**—The ability of a company to make a profit. Profitability is calculated as revenues minus costs.
- **Survivability**—The ability of a company to survive loss due to a risk. Some losses such as fire can be disastrous and 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.

When considering profitability and survivability, you will want to consider the following items:

- **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. This may result in lost opportunities if the money could be used for some other purpose.
- **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/stakeholder confidence**—The value of client and stakeholder confidence is also important. If risks aren't addressed, clients or stakeholders may lose confidence when a threat exploits a vulnerability, resulting in a significant loss to the company.

Consider antivirus software. The cost to install antivirus software on every computer in the organization can be quite high. Every dollar spent reduces the overall profit, and antivirus software doesn't have the potential to add any profit.

However, what's the alternative? If antivirus software is not installed, every system represents a significant risk. If any system becomes infected, a virus could release a worm as a payload and infect the entire network. Databases could be corrupted. Data on file servers could be erased. E-mail servers could crash. The entire business could grind to a halt. If this happens too often or for too long the business could fail.

What Are the Major Components of Risk to an IT Infrastructure?

When you start digging into risk and risk management, you'll realize there is a lot to consider. Luckily, there are several methods and techniques used to break down the topics into smaller chunks.

One method is to examine the seven domains of a typical IT infrastructure. You can examine risks within each domain separately. When examining risks for any domain, you'll look at threats, vulnerabilities and impact. The following sections explore these topics.

Seven Domains of a Typical IT Infrastructure

There are a lot of similarities between different IT organizations. For example, any IT organization will have users and computers. There are seven domains of a typical IT infrastructure.

Figure 1-1 shows the seven domains of a typical IT infrastructure. Refer to this figure when reading through the descriptions of these domains.

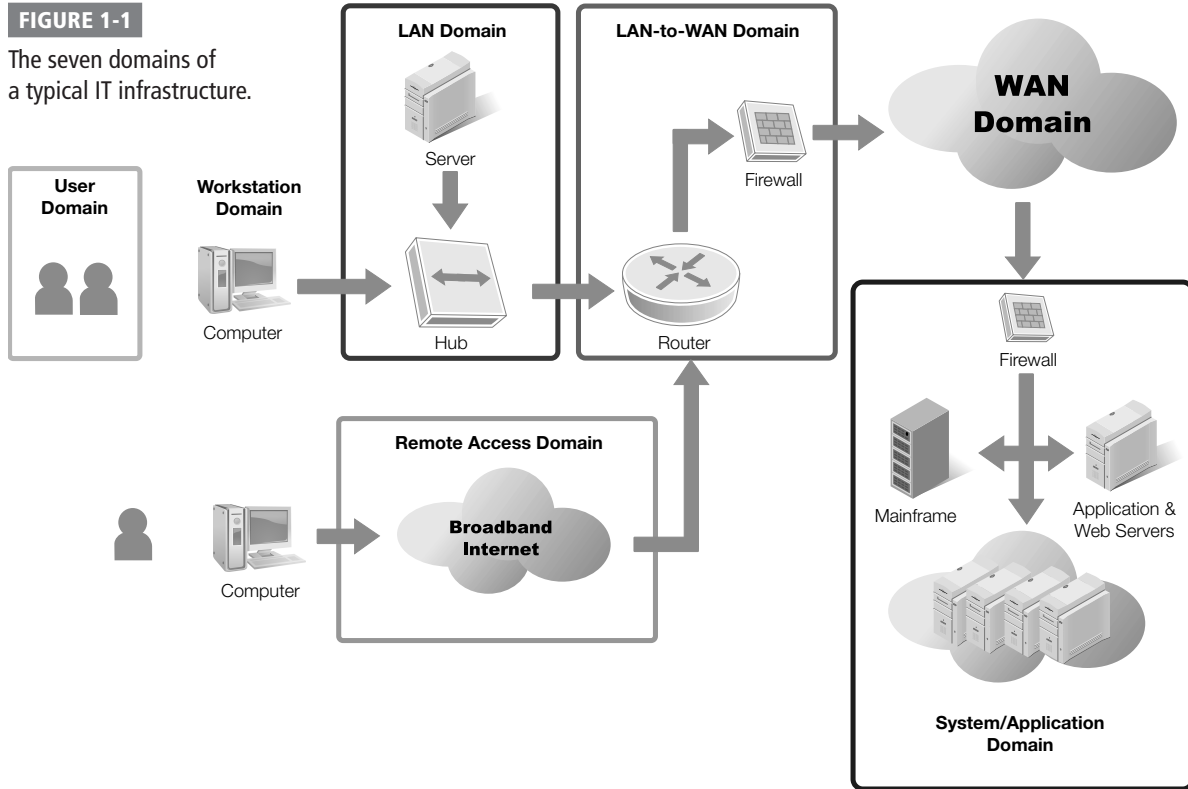
When considering risk management, you can examine each of these domains separately. Each domain represents a possible target for an attacker. Some attackers have the skill and aptitude to con users so they focus on the User Domain. Other attackers may be experts in specific applications so they focus on the System/Application Domain.

NOTE

These seven domains are also explored in Chapters 7, 8, and 10. Chapter 7 covers these domains as they relate to asset and inventory management. Chapter 8 covers them as they relate to threat assessments. Chapter 10 covers them as they relate to risk management.

FIGURE 1-1

The seven domains of a typical IT infrastructure.



An attacker only needs to be able to exploit vulnerabilities in one domain. However, a business 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 includes people. They can be users, employees, contractors, or consultants. The old phrase 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.

You could have the strongest technical and physical security available. However, if personnel don't understand the value of security, the security can be bypassed. For example, technical security can require strong, complex passwords that can't be easily cracked. However, a social engineer can convince an employee to give up the password. Additionally, users may simply write their password down. Some users assume that no one will ever think of looking at the sticky note under their keyboard.

Users can visit risky Web sites, and download and execute infected software. They may unknowingly bring viruses from home via universal serial bus (USB) thumb drives. When they plug in the USB drive the work computer becomes infected. This in turn can infect other computers and the entire network.

Demystifying Social Engineering

Social engineering is a common technique used to trick people into revealing sensitive information. Leonardo DiCaprio played Frank Abagnale in the movie *Catch Me If You Can*, which demonstrated the power of social engineering. A social engineer doesn't just say "give me your secrets." Instead, the attacker uses techniques such as flattery and conning.

A common technique used in vulnerability assessments is to ask employees to give their user name and password. The request may come in the form of an e-mail, a phone call, or even person-to-person.

One common method used in vulnerability assessments is to send an e-mail requesting a user name and password. The e-mail is modified so that it looks as if it's coming from an executive. The e-mail adds a sense of urgency and may include a reference to an important project. From the user's perspective here's what they receive:

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 e-mail with your user name and password. We must complete this test today so please respond as soon as you receive this e-mail.

Thanks for your assistance.

When employees are trained to protect their password, 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.

Workstation Domain

The workstation is the end user's computer. The workstation is susceptible to malicious software, also known as malware. The workstation is vulnerable if it is not kept up to date with recent patches.

If antivirus software isn't installed, the workstation is also vulnerable. If a system is infected, the malware can cause significant harm. Some malware infects a single system. Other malware releases worm components that can spread across the network.

Antivirus companies regularly update virus definitions as new malware is discovered. In addition to installing the antivirus software, companies must also update software regularly with new definitions. If the antivirus software is installed and up to date, the likelihood of a system becoming infected is reduced.

Bugs and vulnerabilities are constantly being discovered in operating systems and applications. Some of the bugs are harmless. Others represent significant risks.

Microsoft and other software vendors regularly release patches and fixes that can be applied. When systems are kept updated, these fixes help keep the systems protected. When systems aren't updated, the threats can become significant.

LAN Domain

The LAN Domain is the area that is inside the firewall. It can be a few systems connected together in a small home office network. It can also be a large network with thousands of computers. Each individual device on the network must be protected or all devices can be at risk.

Network devices such as hubs, switches, and routers are used to connect the systems together on the local area network (LAN). The internal LAN is generally considered a trusted zone. Data transferred within the LAN isn't protected as thoroughly as if it were sent outside the LAN.

NOTE

Many organizations outlaw the use of hubs within the LAN. Switches are more expensive. However, they reduce the risk of sniffing attacks.

As an example, sniffing attacks occur when an attacker uses a protocol analyzer to capture data packets. A protocol analyzer is also known as a sniffer. An experienced attacker can read the actual data within these packets.

If hubs are used instead of switches, there is an increased risk of sniffing attacks. An attacker can plug into any port in the building and potentially capture valuable data.

If switches are used instead of hubs, the attacker must have physical access to the switch to capture the same amount of data. Most organizations protect network devices in server rooms or wiring closets.

LAN-to-WAN Domain

The LAN-to-WAN Domain connects the local area network to the wide area network (WAN). The LAN Domain is considered a trusted zone since it is controlled by a company. The WAN Domain is considered an untrusted zone because it is not controlled and is accessible by attackers.

The area between the trusted and untrusted zones is protected with one or more firewalls. This is also called the boundary, or the edge. Security here is referred to as boundary protection or edge protection.

The public side of the boundary is often connected to the Internet and has public Internet Protocol (IP) addresses. These IP addresses are accessible from anywhere in the world, and attackers are constantly probing public IP addresses. They look for vulnerabilities and when one is found, they pounce.

A high level of security is required to keep the LAN-to-WAN Domain safe.

Remote Access Domain

Mobile workers often need access to the private LAN when they are away from the company. Remote access is used to grant mobile workers this access. Remote access can be granted via direct dial-up connections or using a virtual private network (VPN) connection.

A VPN provides access to a private network over a public network. The public network used by VPNs is most commonly the Internet. Since the Internet is largely untrusted and has known attackers, remote access represents a risk. Attackers can access unprotected connections. They can also try to break into the remote access servers. Using a VPN is an example of a control to lessen the risk. But VPNs have their vulnerabilities, too.

Vulnerabilities exist at two stages of the VPN connection:

- The first stage is authentication. Authentication is when the user provides credentials to prove identity. If these credentials can be discovered, the attacker can later use them to impersonate the user.
- The second stage is when data is passed between the user and the server. If the data is sent in clear text, an attacker can capture and read the data.

WAN Domain

For many businesses, the WAN is the Internet. However, a business can also lease semiprivate lines from private telecommunications companies. These lines are semiprivate because they are rarely leased and used by only a single company. Instead, they are shared with other unknown companies.

As mentioned in the LAN-to-WAN Domain, the Internet is an untrusted zone. Any host on the Internet with a public IP address is at significant risk of attack. Moreover, it is fully expected that any host on the Internet will be attacked.

Semiprivate lines aren't as easily accessible as the Internet. However, a company rarely knows who else is sharing the lines. These leased lines require the same level of security provided to any host in the WAN Domain.

A significant amount of security is required to keep hosts in the WAN Domain safe.

System/Application Domain

The System/Application Domain refers to servers that host server-level applications. Mail servers receive and send e-mail for clients. Database servers host databases that are accessed by users, applications, or other servers. Domain Name System (DNS) servers provide names to IP addresses for clients.

You should always protect servers using best practices: Remove unneeded services and protocols. Change default passwords. Regularly patch and update the server systems. Enable local firewalls.

One of the challenges with servers in the System/Application Domain is that the knowledge becomes specialized. People tend to focus on areas of specialty. For example, common security issues with an e-mail server would likely be known only by technicians who regularly work with the e-mail servers.

NOTE

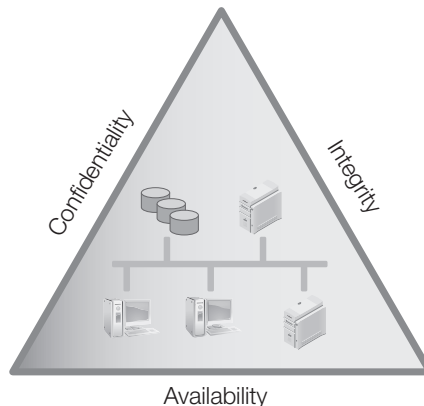
VPN connections use tunneling protocols to reduce the risk of data being captured. A tunneling protocol will encrypt the traffic sent over the network. This makes it more difficult for attackers to capture and read data.

TIP

You should lock down a server using the specific security requirements needed by the hosted application. An e-mail server requires one set of protections while a database server requires a different set.

FIGURE 1-2

Security objectives for information and information systems.



Threats, Vulnerabilities, and Impact

When a threat exploits a vulnerability it results in a loss. The **impact** identifies the severity of the loss.

A threat is any circumstance or event with the potential to cause a loss. You can also think of a threat as any activity that represents a possible danger. Threats are always present and cannot be eliminated, but they may be controlled.

Threats have independent probabilities of occurring that often are unaffected by an organizational action. As an example, an attacker may be an expert in attacking Web servers hosted on Apache. There is very little a company can do to stop this attacker from trying to attack. However, a company can reduce or eliminate vulnerabilities to reduce the attacker's chance of success.

Threats are 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 are common security objectives for information systems.

Figure 1-2 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.

NOTE

Confidentiality, integrity, and availability are often referred to as the security triad.

- **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.

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

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

Consider 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 becomes vulnerable.

The impact is the amount of the loss. The loss 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, you can use the purchase value or the replacement value. 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 describe the impact. You can describe losses in relative terms such as high, medium, or low. As an example, NIST SP 800-30 suggests the following impact terms:

High Impact—If a threat exploits the vulnerability it may:

- Result in the costly loss of major assets or resources
- Significantly violate, harm, or impede an organization's mission, reputation, or interest
- Or, result in human death or serious injury.

Medium Impact—If a threat exploits the vulnerability it may:

- Result in the costly loss of assets or resources
- Violate, harm, or impede an organization's mission, reputation, or interest
- Or, result in human injury.

Low Impact—If a threat exploits the vulnerability it may:

- Result in the loss of some assets or resources
- Or, noticeably affect an organization's mission, reputation, or interest.

Risk Management and Its Importance to the Organization


Risk management is the practice of identifying, assessing, controlling, and mitigating risks. Threats and vulnerabilities are key drivers of risk. Identifying the threats and vulnerabilities that are relevant to the organization is an important step. You can then take action to reduce potential losses from these risks.

It's important to realize that risk management isn't intended to be risk elimination. That isn't a reasonable goal. Instead, risk management attempts to identify the risks that can be minimized and implement controls to do so. Risk management includes several elements:

**TIP**

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

- **Risk assessment**—Risk management starts with a **risk assessment** or risk analysis. There are multiple steps to a risk assessment:

 **NOTE**

Risk assessment is covered in more depth in chapters 5 and 6.

- Identify the IT assets of an organization and their value. This can include data, hardware, software, services, and the IT infrastructure.
 - Identify threats and vulnerabilities to these assets. Prioritize the threats and vulnerabilities.
 - Identify the likelihood a vulnerability will be exploited by a threat. These are your risks.
 - Identify the impact of a risk. Risks with higher impacts should be addressed first.
- **Identify risks to manage**—You can choose to avoid, transfer, mitigate, or accept risks. The decision is often based on the likelihood of the risk occurring, and the impact it will have if it occurs.
 - **Selection of controls**—After you have identified what risks to address, you can identify and select control methods. Control methods are also referred to as countermeasures. **Controls** are primarily focused on reducing vulnerabilities and impact.
 - **Implementation and testing of controls**—Once the controls are implemented, you can test them to ensure they provide the expected protection.
 - **Evaluation of controls**—Risk management is an ongoing process. You should regularly evaluate implemented controls to determine if they still provide the expected protection. Evaluation is often done by performing regular vulnerability assessments.

How Risk Affects an Organization's Survivability

Profitability and survivability were presented earlier in the chapter. You should also consider them when identifying which risks to manage. Consider both the cost to implement the control and the cost of not implementing the control. As mentioned previously, spending money to manage a risk rarely adds profit. The important point is that spending money on risk management can help ensure a business's survivability.

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

Imagine that a business spends \$15,000 a year on data backups. This cost will not increase revenue or profits. Imagine that 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. The next year, data could be lost, causing the company to fail.

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

On the other hand, imagine a company with \$100,000 in annual profits. They choose not to spend the \$15,000 on backups. Then a virus spreads through the enterprise, destroying all customer and accounting data. The company no longer has reliable records of accounts receivable. No one has access to the customer base. This can be a business-ending catastrophe.

Reasonableness

A company doesn't need to manage every possible risk. Some risks are reasonable to manage while others are not.

Reasonableness is a test that can be applied to risk management to determine if the risk should be managed. It's derived from the reasonable-person standard in law. In short, you should answer this question. "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 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 a hurricane is not. So, for San Francisco, the risk of a hurricane is readily accepted while risk of an earthquake may not be accepted.

Balancing Risk and Cost

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

Table 1-1 shows an example of how the relative values can be assigned. This matrix was derived from NIST SP 800-30. Likelihood values are shown vertically, while impact values are shown horizontally. If a threat has a 10 percent likelihood of occurring it is assigned a value of Low. If the value is between 10 and 50 percent, the value is medium.

	LOW IMPACT 10	MEDIUM IMPACT 50	HIGH IMPACT 100
High threat likelihood 100 percent (1.0)	$10 \times 1 = 10$	$50 \times 1 = 50$	$100 \times 1 = 100$
Medium threat likelihood 50 percent (.50)	$10 \times .50 = 5$	$50 \times .50 = 25$	$100 \times .50 = 50$
Low threat likelihood 10 percent (.10)	$10 \times .10 = 1$	$50 \times .10 = 5$	$100 \times .10 = 10$

TIP

You can create a more detailed likelihood-impact matrix. For example, instead of assigning values of low, medium, and high for the threat likelihood, you can assign actual percentages. This allows greater separation between the categories. Similarly, you can assign any number within a range to the impact. The matrix in the table uses a range of 10, 50, and 100, but you could use any numbers between 1 and 100, if desired.

If the value is between 51 and 100, the value is high. Similarly, the impact can be ranked as low, medium, and high.

The potential of some risks to occur is very high and the impact is high giving you 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 if a fire occurs. Insurance is also purchased to reduce the impact if a fire does cause damage.

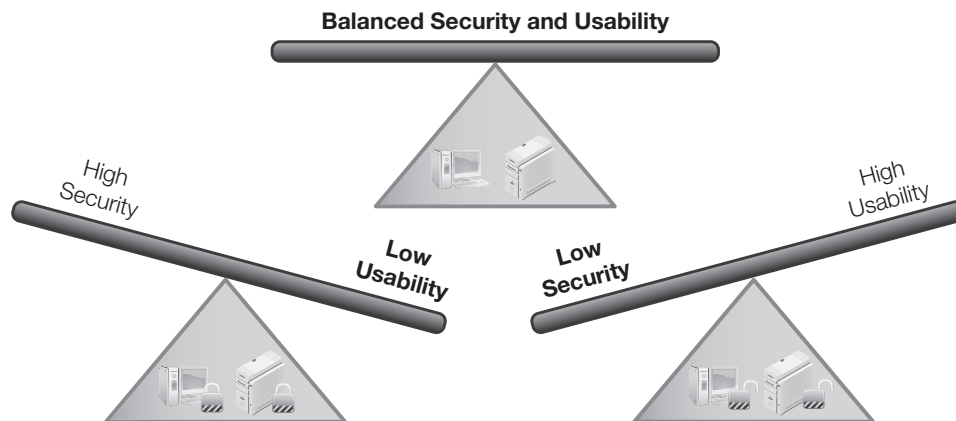
Role-Based Perceptions of Risk

Ideally, all personnel within an organization will readily understand the threat to a company's health if risk is not managed. Unfortunately, risks and risk management are often perceived quite differently.

One of the challenges with effective risk management is achieving a proper balance between security and usability. Consider Figure 1-3. In the diagram on the left, the computers are completely locked down with a high level of security. Users are unable to use them to adequately perform their job. On the right, the computers are easy to use but security is neglected. In the middle, a balance between the two has been achieved.

FIGURE 1-3

Balancing security and usability in an organization.



Balanced security rarely satisfies everyone. Security personnel want to lock systems down tighter. End users find the security controls inconvenient and want more usability. It is common for individuals in the following roles to have different perceptions of risk:

- **Management**—Management is concerned mostly with profitability and survivability. Since attacks can result in loss of confidentiality, integrity, or availability, management is willing to spend money to mitigate risks. However, their view of the risk is based on the costs of the risk and the costs of the controls. Management needs accurate facts to make decisions on which controls to implement to protect company assets.
- **System administrator**—Administrators are responsible for protecting the IT systems. When they understand the risks, they often want to lock systems down as tight as possible. Administrators are often highly technical individuals. System administrators sometimes lose sight of the need to balance security costs with profitability.
- **Tier 1 administrator**—Tier 1 administrators are the first line of defense for IT support (thus the “tier 1” part of the name). When a user needs assistance, a tier 1 administrator is often called. They may be more concerned with usability than security or profitability. These administrators are given limited administrative permissions. They often view the security controls as hindrances to perform 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. Many developers have adopted a secure computing mindset. They realize that security needs to be included from the design stage all the way 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, resulting in the release of vulnerable software.
- **End user**—End users simply want the computer to work for them. They are most concerned with usability. They 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, USB thumb drives often transport viruses without the user’s knowledge. Companies frequently implement policies restricting the use of thumb drives. When a user needs to transfer a file from one computer to another, the USB thumb drive can be tempting.

 **TIP**

You can restrict the use of thumb drives through a written policy telling people not to use them. You can also use technical controls to prevent use of thumb drives. 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.

You can address the perceptions of these different role holders through targeted training. Some training can include all employees; other training should be targeted to specific roles. Targeted training helps each role holder 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 the 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. The lock 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. In addition to purchasing the lock, steps need to be taken to train the users.

Risk Identification Techniques

You learned about risk and losses earlier in this chapter. Risk is the likelihood that a loss will occur. Losses occur when a threat exposes a vulnerability. In order to identify risks, you'll need to take three steps:

- Identify threats
- Identify vulnerabilities
- Estimate the likelihood of a threat exploiting a vulnerability

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 your password or a company's "secret formula."
- **Loss of integrity**—An e-mail message is modified in transit, a virus infects a file, or someone makes unauthorized changes to a Web site.
- **Loss of availability**—An e-mail server is down and no one has e-mail access, or a file server is down so data files aren't available.

"Threat identification" is the process of creating a list of threats. This list attempts to identify all the possible threats to an organization. This is no small task. The list can be extensive.

Threats are often considered 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 error 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 only analyzed logically.

Some examples of threats to an organization include:

- An unauthorized employee trying to access data
- Any type of malware
- An attacker defacing a Web site
- 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

 **TIP**

A denial of service (DoS) attack is an attack that attempts to disrupt a service. A DoS attack results in the service being unavailable. A distributed denial of service (DDoS) attack originates from multiple attackers.

All these threats represent possible risks if they expose vulnerabilities.

Of course, you will identify different threats and vulnerabilities depending on the organization. Every organization has threats and vulnerabilities specific to them. In fact, a business with multiple locations may have some threats and vulnerabilities unique to one location.

Identifying Vulnerabilities

You learned earlier that a vulnerability is a weakness. When a threat occurs, if there is a vulnerability the weakness is apparent. However, before threats occur, you'll have to dig a little to identify the weaknesses. Luckily, most organizations have a lot of sources which can help you.

Some of the sources you can use are:

- **Audits**—Many organizations are regularly audited. Systems and processes are checked to verify a company complies with existing rules and laws. At the completion of an audit, a report is created. These reports list findings which 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 logs can be used to identify threats. Audit logs can determine if users are accessing sensitive data. Firewall logs can identify traffic that is trying to breach the network. Firewall logs can also identify computers taken over by malware and acting as zombies. DNS logs can identify unauthorized transfer of data.
- **Prior events**—Previous security incidents are excellent sources of data. As evidence of risks which 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, employees are sometimes 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.

 **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.”

- **Trouble reports**—Most companies use databases to document trouble calls. These databases can contain a wealth of information. With a little bit of analysis, you can use them to identify trends and weaknesses.
- **Incident response teams**—Some companies have incident response teams. These teams will investigate all the security incidents within the company. You can interview team members and get a wealth of information. These teams 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. These domains 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 gives you some examples in each of these domains:

- **User Domain**—Social engineering represents a big vulnerability. 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? 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 Web sites, 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 a SQL injection attack, the attacker can read the entire database. SQL injection attacks can also modify data in the database.

TIP

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

TIP

A "SQL injection attack" tries to access data from Web sites. SQL statements are entered into text boxes. If the Web site isn't programmed defensively, these SQL statements can be executed against a database. Some programs are available that can launch a SQL injection attack and retrieve an entire database.

This list certainly isn't complete. The number of vulnerabilities discovered in IT is constantly growing. The MITRE Corporation catalog **Common Vulnerabilities and Exposures (CVE)** includes more than 40,000 items.

Using Reason When Identifying Vulnerabilities

Reasonableness was covered earlier in this chapter. As a reminder, reasonableness answers the question, "Would a reasonable person be expected to manage this risk?" In this context, you can think of it as, "Would a reasonable person be expected to reduce this vulnerability?"

You should focus on vulnerabilities within the organization or within the system being evaluated. External vulnerabilities are often not addressed. For example, a server will likely fail if air conditioning fails. You would address this when identifying vulnerabilities for a server room. You wouldn't address for each of the 50 servers in the server room. Similarly, the commercial power may fail. You may address this by having uninterruptible power supplies (UPS) and generators. However, you don't need to identify alternatives for the commercial power company.

TABLE 1-2 Risk and trust levels of common network zones.

THREAT	VULNERABILITY	IMPACT
An unauthorized employee tries to access data hosted on a server.	The organization doesn't use 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, this could impact morale and productivity.
Any type of malicious software, 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 Web site.	The Web site isn't protected.	Depending on how the attacker modifies the Web site, 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.

Pairing Threats with Vulnerabilities

The third step when identifying risks is to pair the threats with vulnerabilities. Threats are matched to existing vulnerabilities to determine the likelihood of a risk.

The "Identifying Threats" section listed several threats. Table 1-2 takes a few of those threats and matches them to vulnerabilities to identify 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. Compare this to the formula for area: $\text{Area} = \text{Length} \times \text{Width}$. Length has a numerical value. Width has a numerical value. The result is a number for Area.

Threat and vulnerability often don't have numerical values. The formula isn't intended to give a number as a result. Instead, it is designed to show the relationship between the two.

If you can identify the value of the asset, the formula is slightly modified to:

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

Risk Management Techniques

After risks have been identified, you need to decide what you want to do about them. Risk management can be thought of as handling risk. It's important to realize that risk management is not risk elimination. A business that doesn't take any risks doesn't stay in business long. The cost to eliminate all risks will 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. They include:

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

When deciding how to handle a risk you can choose to **avoid**, **transfer**, **mitigate**, or **accept** the risk. These techniques are explained in the following section.

Avoidance

One of the ways you manage risk is by simply avoiding it. The primary reason to avoid a risk is that 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. This 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. The cost to move the data center will be high. However, if the risk is unacceptable and the value of the data center is higher it makes sense.

Transfer

You can transfer risk by shifting responsibility to another party. This is most commonly done by purchasing insurance. It can also be done by outsourcing the activity.

- **Insurance**—You purchase insurance to protect your company 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, your company may want to host a Web site on the Internet. The company can host the Web site with a Web hosting provider. Your company and the provider can agree on who assumes responsibility for security, backups, and availability.

Mitigation

You reduce risk by reducing vulnerabilities, and risk mitigation is the primary strategy in this process. Risk mitigation is also known as reduction or treatment.

You reduce vulnerabilities by implementing controls or countermeasures. The cost of a control should not exceed the benefit. Determining costs and benefits often requires a cost-benefit analysis, which is covered later in this chapter.

Some examples of mitigation steps are:

TIP

Controls are often referred to as either preventive or detective. A “preventive control” attempts to deter or 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.

- **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 offsite, and test the backups.
- **Add fault tolerance**—Use Redundant Array of Independent Disks (RAID) for important data stored on disks. Use failover clusters to protect servers.
- **Modify the technical environment**—Increase security on the firewalls. Add intrusion detection systems. 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. Consider the following two formulas.

- **Attacker’s cost < attacker’s gain**—When this is true, it 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 your company sends data across the network in clear text, it 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 too time-consuming for the attacker to crack it.

Acceptance

You can also choose to accept a risk. A company can evaluate a risk, understand the potential loss, and choose to accept it. This is commonly done when the cost of the control outweighs the potential loss.

For example, consider the following scenario: 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 \times 12 / 365 / 24 = \1.37 .)

The decision to accept a loss becomes easier if you have evaluated the costs against the benefits, which is known as a “cost-benefit analysis.” A cost-benefit analysis is useful when choosing any of the techniques to manage risk.

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.

Cost-Benefit Analysis

You perform a **cost-benefit analysis (CBA)** 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, you would spend \$10,000 to save \$1 million. This makes sense.

A CBA starts by gathering data to identify the costs of the controls and benefits gained if they are implemented.

- **Cost of the control**—This includes the purchase costs plus the operational costs over the lifetime of the control.
- **Projected benefits**—This includes the potential benefits gained from implementing the control. You identify these benefits by examining the costs of the loss and how much the loss will be reduced if the control is 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. The benefit of the control is \$90,000.

You can use the following formula to determine if the control should be used:

$$\text{Loss before control} - \text{loss after control} = \text{cost of control}$$

Imagine the company lost \$100,000 last year without any controls implemented. You estimate you’ll lose \$10,000 a year if the control is implemented. The cost of the control is estimated at \$10,000. The formula is:

$$\$100,000 - \$10,000 \text{ (cost of control)} - \$10,000 \text{ (expected residual loss)} = \$80,000$$

This represents a benefit of \$80,000.

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

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

- Costs to train employees
- Costs for ongoing maintenance
- Software and hardware renewal costs

If the costs outweigh the benefits, the control may not be implemented. Instead, the risk could be accepted, transferred or avoided.

Residual Risk

Residual risk is the risk that remains after you apply controls. It's not feasible to eliminate all risks. Instead, you take steps 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:

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

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

You can calculate residual risk with the following formula:

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

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



CHAPTER SUMMARY

Risks occur when threats exploit vulnerabilities, resulting in a loss. The loss can compromise business functions and business assets. Losses also drive business costs. Risk management helps a company identify risks that need to be reduced. The first steps in risk management are to identify threats and vulnerabilities. These can then be paired to help determine the severity of the risk.

You can manage risks by choosing one of four techniques: A risk can be avoided, transferred, mitigated, or accepted. The primary risk management technique is risk mitigation. Risk mitigation is also known as risk reduction or risk treatment. You reduce vulnerabilities by implementing controls.



KEY CONCEPTS AND TERMS

Accept	Impact	Risk assessment
Availability	Intangible value	Risk management
Avoid	Integrity	Survivability
Common Vulnerabilities and Exposures (CVE)	Mitigate	Tangible value
Confidentiality	Profitability	Threat
Control	Reasonableness	Total risk
Cost-benefit analysis (CBA)	Residual risk	Transfer
	Risk	Vulnerability

**CHAPTER 1 ASSESSMENT**

1. Which one of the following properly defines risk?
 - A. Threat \times Mitigation
 - B. Vulnerability \times Controls
 - C. Controls $-$ Residual Risk
 - D. Threat \times Vulnerability
2. Which one of the following properly defines total risk?
 - A. Threat $-$ Mitigation
 - B. Threat \times Vulnerability \times Asset Value
 - C. Vulnerability $-$ Controls
 - D. Vulnerability \times Controls
3. You can completely eliminate risk in an IT environment.
 - 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. Eliminate losses related to employee actions
 - B. Eliminate losses related to risk
 - C. Reduce losses related to residual risk
 - D. 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 a risk management?
 - A. Identify the correct cost balance between risk and controls
 - B. Eliminate risk by implementing controls
 - C. Eliminate the loss associated with risk
 - D. 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. This is known as risk _____.
13. What can you do to manage risk? (Select three.)
 - A. Accept
 - B. Transfer
 - C. Avoid
 - D. Migrate
14. You have applied controls to minimize risk in the environment. 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 management
 - D. Security personnel