PART I

The Need for Information Security

CHAPTER 1 Information Systems Security 2

CHAPTER 2 The Internet of Things is Changing How We Live 47

CHAPTER 3 Malicious Attacks, Threats, and Vulnerabilities 72

CHAPTER 4 The Drivers of the Information Security Business 112

CHAPTER

1

Information Systems Security

THE INTERNET HAS CHANGED DRAMATICALLY from its origins. It has grown from a tool used by a small number of universities and government agencies to a worldwide network with more than 3 billion users. As it has grown, it has changed the way people communicate and do business, bringing many opportunities and benefits. Today the Internet continues to grow and expand in new and varied ways. It supports innovation and new services such as IP mobility and smartphone connectivity. When the Internet started, the majority of connected devices were solely computers, whether for personal use or within a company. In the most recent years, however, an increasing variety of devices beyond computers, including smartphones, smart cars, appliances, vending machines, smart homes, and smart buildings, can connect and share data.

The Internet as we know it today is expanding rapidly as the **Internet of Things (IoT**) takes over and impacts our day-to-day lives. Although the Internet officially started back in 1969, the extent to which people depend on the Internet is new. Today, people interact with the Internet and cyberspace as part of normal day-to-day living. This includes personal use and business use. Users must now address issues of privacy data security and business data security. Security threats can come from either personal or business use of your Internet-connected device. Intelligent and aggressive cybercriminals, terrorists, and scam artists lurk in the shadows. Connecting your computers or devices to the Internet immediately exposes them to attack. These attacks result in frustration and hardship. Anyone whose personal information has been stolen (called **identity theft**) can attest to that. Worse, attacks on computers and networked devices are a threat to the national economy, which depends on **e-commerce**. Even more important, cyberattacks threaten national security. For example, terrorist attackers could shut down electricity grids and disrupt military communication.

You can make a difference. The world needs people who understand computer security and who can protect computers and networks from criminals and terrorists. Remember, it's all about securing your sensitive data. If you have sensitive data, you must protect it. To get you started, this chapter gives an overview of information systems security concepts and terms that you must understand to stop cyberattacks.

Chapter 1 Topics

This chapter covers the following topics and concepts:

- What unauthorized access and data breaches are
- What information systems security is
- What the tenets of information systems security are
- What the seven domains of an IT infrastructure are
- What the weakest link in an IT infrastructure is
- How an IT security policy framework can reduce risk
- How a data classification standard affects an IT infrastructure's security needs

Chapter 1 Goals

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

- Describe how unauthorized access can lead to a data breach
- Relate how availability, integrity, and confidentiality requirements affect the seven domains of a typical IT infrastructure
- Describe the risk, threats, and vulnerabilities commonly found within the seven domains
- Identify a layered security approach throughout the seven domains
- Develop an IT security policy framework to help reduce risk from common threats and vulnerabilities
- Relate how a data classification standard affects the seven domains

Information Systems Security

Today's **Internet** is a worldwide network with more than 2 billion users. It includes almost every government, business, and organization on Earth. However, having that many users on the same network wouldn't solely have been enough to make the Internet a game-changing innovation. These users needed some type of mechanism to link documents and resources across computers. In other words, a user on computer A needed an easy way to open a document on computer B. This need gave rise to a system that defines how documents and resources are related across network machines. The name of this system is the **World Wide Web (WWW)**. You may know it as **cyberspace** or simply as the Web. Think of it this way: The Internet links communication networks to one another. The Web is the connection of websites, webpages, and digital content on those networked computers. Cyberspace is all the accessible users, networks, webpages, and applications working in this worldwide electronic realm.

Recent Data Breaches in the United States (2013–2015)

The past couple of years have seen a dramatic increase in the number of reported **data breaches** in the United States. Both the public sector and the private sector have fallen victim. **TABLE 1-1** lists a summary of recent data breaches, the affected organization, and the impact of the data breach to that organization.

TABLE 1-1 Recent data breaches in the United States, 2013–2015.

ORGANIZATION	DATA BREACH	IMPACT OF DATA BREACH
Adobe Systems Incorporated: Software subscription database	In a breach on October 3, 2013, Adobe announced that hackers had published data for 150 million accounts and had stolen encrypted customer credit card data. Logon credentials were also compromised for an undetermined number of Adobe user accounts.	The hackers stole 3 million credit card records and accessed 160,000 Social Security numbers (SSNs). Adobe has offered a year's worth of credit monitoring to customers affected by the breach.
Anthem, Inc.: Blue Cross Blue Shield customer database	On February 4, 2015, Anthem disclosed that criminal hackers had broken into its servers and potentially stolen from its servers over 37.5 million records that contain personally identifiable information. On February 24, 2015, Anthem raised the number of victims to 78.8 million people whose personal information was affected. The data breach extended into multiple brands Anthem uses to market its health care plans, including Anthem Blue Cross, Anthem Blue Cross and Blue Shield, Blue Cross and Blue Shield of Georgia, Empire Blue Cross and BlueShield, Amerigroup, Caremore, and UniCare.	Individuals whose data was stolen could have problems resulting from identity theft for the rest of their lives. Anthem had a $100 million insurance policy covering cyberattacks from American International Group One.

ORGANIZATION	DATA BREACH	IMPACT OF DATA BREACH
Excellus BlueCross BlueShield: Blue Cross Blue Shield customer database	Personal data from more than 10 million members became exposed after the company's IT systems were breached, beginning as far back as December 2013. Among the affected individuals in the Excellus breach are members of other Blue Cross Blue Shield plans who sought treatment in the 31-county upstate New York service area of Excellus, according to the company. Compromised data includes names, addresses, birthdates, SSNs, health plan ID numbers, and financial account information, as well as claims data and clinical information.	The suit against Excellus alleges that the health insurer failed to fulfill its legal duty to protect the sensitive information of its customers and those customers whose data were stored in its systems. In addition, the suit alleges that Excellus knew about the security breach for over one month before it publicly disclosed the incident.
Hilton Hotels & Resorts: Travel industry customer and credit card database	After multiple banks suspected a credit card breach at Hilton properties across the country, Hilton acknowledged an intrusion involving malicious software had been found on some point-of-sale systems. Hilton said the stolen data included cardholder names, payment card numbers, security codes, and expiration dates, but no addresses or personal identification numbers.	Hilton identified and took action to eradicate unauthorized malware that targeted payment card information and strengthened its security. The company offered one year of free credit monitoring to affected customers.
Target Corp.: Customer and credit card database of the nationwide retailer	In December 2013, a data breach of Target's systems affected up to 110 million customers. Compromised customer information included names, phone numbers, email, and mailing addresses.	Target agreed to reimburse some costs that financial institutions incurred as a result of the breach, but the retailer has failed to reach a settlement with MasterCard over the resulting dispute.

(*continues*)

TABLE 1-1 Recent data breaches in the United States, 2013–2015. (*Continued*)

ORGANIZATION	DATA BREACH	IMPACT OF DATA BREACH
Experian Information Solutions, Inc., and T-Mobile USA, Inc.: Database of T-Mobile customers applying for credit	On September 15, 2015, Experian discovered that attackers had breached one North American business unit server containing the personal data of about 15 million T-Mobile customers who had applied for credit. T-Mobile shared this information with Experian to process credit checks or provide financing. Social Security and credit card information was compromised. The Internal Revenue Service (IRS) has confirmed that 13,673 U.S. citizens have been victimized through the filing of $65 million in fraudulent individual income tax returns as a result of this data breach.	T-Mobile is suffering reputational and financial damage because of the actions of a third-party partner and not its own, notwithstanding the carrier's choice of business partners.
Sony Pictures Entertainment: Confidential files, emails, and employee data	On November 24, 2014, a hacker group identifying itself with the name Guardians of Peace leaked confidential data from the Sony Pictures film studio. The data leak included personal information about Sony Pictures employees and their families, emails between employees, information about Sony executive salaries, copies of then-unreleased Sony films, and other information. In December, the FBI identified the Guardians of Peace as acting on behalf of the North Korean government.	On January 2, 2015, U.S. President Barack Obama issued an executive order enacting additional sanctions against the North Korean government and a North Korean arms dealer, specifically citing this cyberattack and ongoing North Korean policies. Obama also issued a legislative proposal to Congress to update current laws to better respond to cybercrimes like the Sony hack and to be able to prosecute such crimes compatibly with similar offline crimes while protecting citizens' privacy.

ORGANIZATION	DATA BREACH	IMPACT OF DATA BREACH
U.S. Office of Personnel Management : Agency of the U.S. Federal government	In June 2015, the U.S. Office of Personnel Management (OPM) announced that it had been the target of a data breach impacting approximately 22 million people. The data breach was noticed by the OPM in April 2015. Federal officials described it as among the largest breaches of government data in the history of the United States. Information targeted in the breach included personally identifiable information such as SSNs as well as names, dates, and places of birth and addresses. The hack went deeper than initially believed and likely involved theft of detailed security clearance-related background information.	The data breach has created a massive counterintelligence threat that could easily last 40 years. For every nonmarried federal employee in the background investigation database, at least four out of five people will require monitoring. For those who have been married or married more than once, the number of affected people is at least 12 out of 14.
The Wendy's Co.: Customer and credit card database of the nationwide fast-food retailer	After becoming suspicious in December 2015, the Ohio-based burger chain began looking into reports of unusual activity on credit cards used at Wendy's locations across the country. The company hired a team of cybersecurity experts to help assess the damage and is cooperating with law enforcement in a criminal investigation. Customers at as many as 6,000 Wendy's locations may have been affected.	The investigation is new and ongoing, but card breaches are becoming more and more common in the restaurant industry. Restaurant chains are especially susceptible, likely because of their use of outdated technology.

Unfortunately, when you connect to cyberspace, you also open the door to a lot of bad guys. They want to find you and steal your data. Every computer or device that connects to the Internet is at risk, creating an Internet of Things (IoT) that supports users in all aspects of their lives. Like outer space, the maturing Internet is a new frontier. There is no Internet government or central authority. It is full of challenges—and questionable behavior. This questionable behavior is evident given the data breaches we've seen in the past three years alone. In the United States, public and private sectors have been compromised through unauthorized access and data breach attacks. These recent attacks have been committed by individuals, organized cybercriminals, and attackers from other nations. The quantity of cyberattacks on U.S. interests is increasing.

With the Internet of Things (IoT) now connecting personal devices, home devices, and vehicles to the Internet, there are even more data to steal. All users must defend their information from attackers. **Cybersecurity** is the duty of every government that wants to ensure its national security. Data security is the responsibility of every organization that needs to protect its information assets and sensitive data (e.g., SSNs, credit card numbers, and the like). And it's the job of all of us to protect our own data. **FIGURE 1-1** illustrates this new frontier.

The components that make up cyberspace are not automatically secure. These components include cabling, physical networks, operating systems, and software applications that computers use to connect to the Internet. At the heart of the problem is the lack of security in the **Transmission Control Protocol/Internet Protocol (TCP/IP)** communications protocol. This protocol

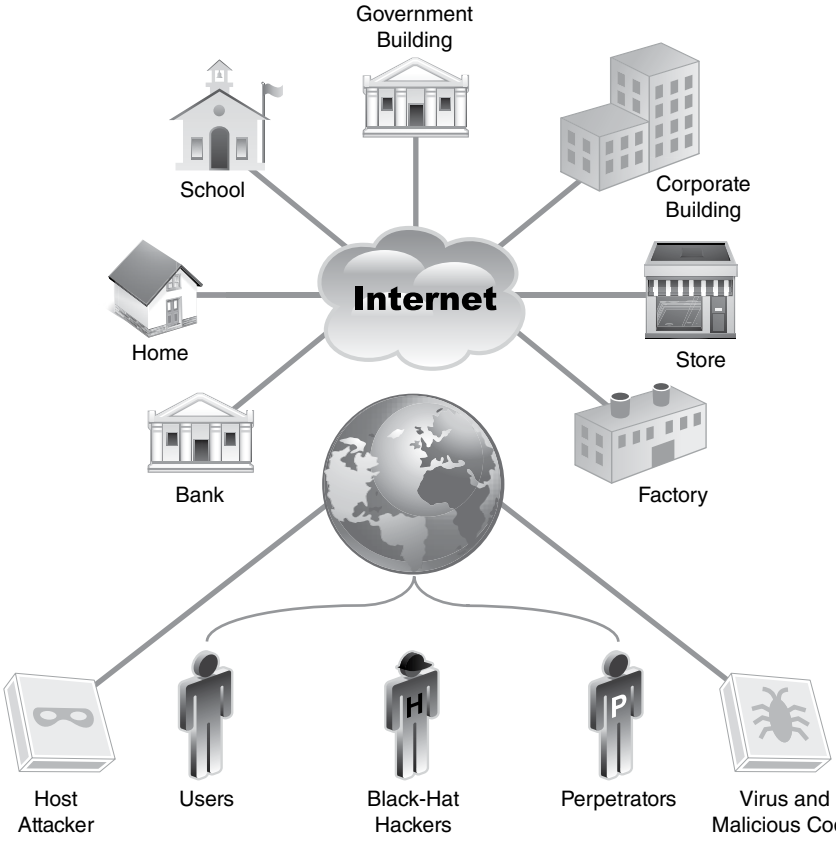
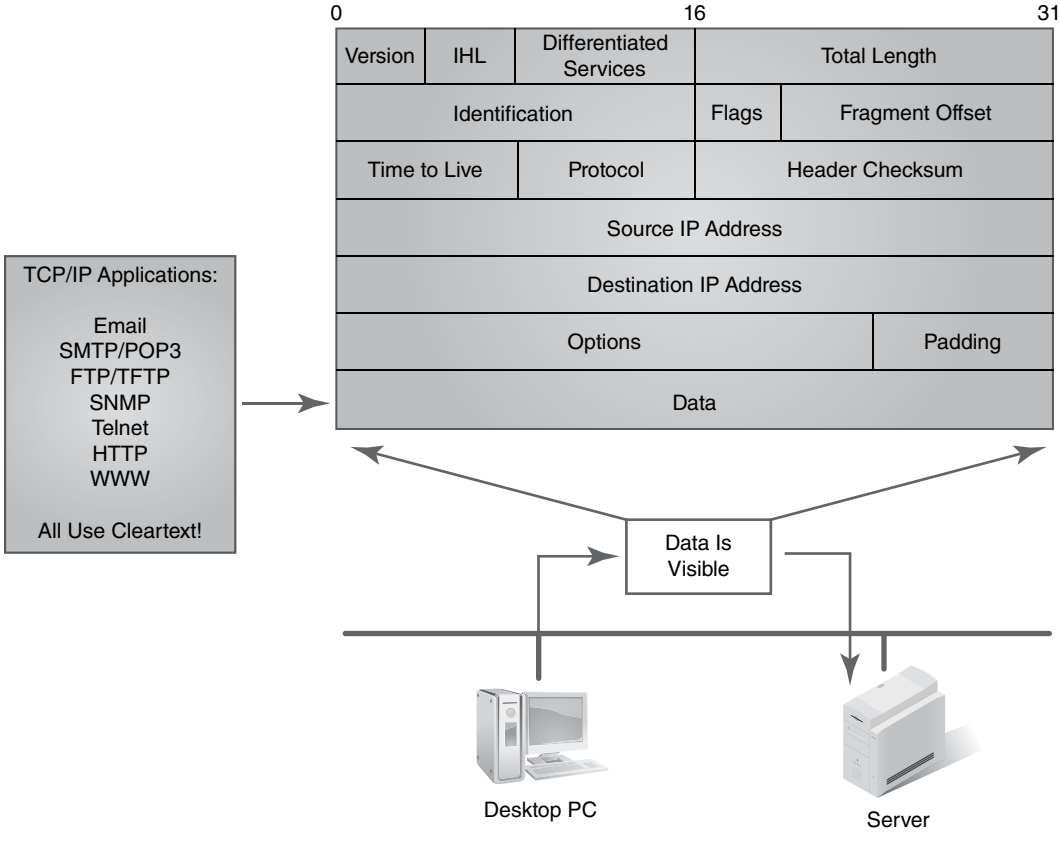


FIGURE 1-1
Cyberspace: the new frontier.

is the language that computers most commonly use to communicate across the Internet. (A **protocol** is a list of rules and methods for communicating.) TCP/IP is not just one protocol but a suite of protocols developed for communicating across a network. Named after the two most important protocols, TCP/IP works together to allow any two computers to communicate. Connecting two or more computers creates a network. TCP/IP breaks messages into chunks, or packets, to send data between networked computers. The problem lies in the fact that data are readable within each IP packet using simple software available to anyone. This readable mode is known as **cleartext**. That means you must hide or encrypt the data sent inside a TCP/IP packet to make the data more secure. FIGURE 1-2 shows the data within the TCP/IP packet structure.

All this raises the question: If the Internet is so unsafe, why did everyone connect to it so readily? The answer is the huge growth of the Web from the mid-1990s to the early 2000s. Connecting to the Internet gave anyone instant access to the Web and its many resources. The appeal of easy worldwide connectivity drove the demand to connect. This demand and subsequent growth helped drive costs lower for high-speed communications. Households, businesses, and governments gained affordable high-speed Internet access. And as wireless and cellular connections have become more common and affordable, it has become easier to

FIGURE 1-2
TCP/IP communications are in cleartext.



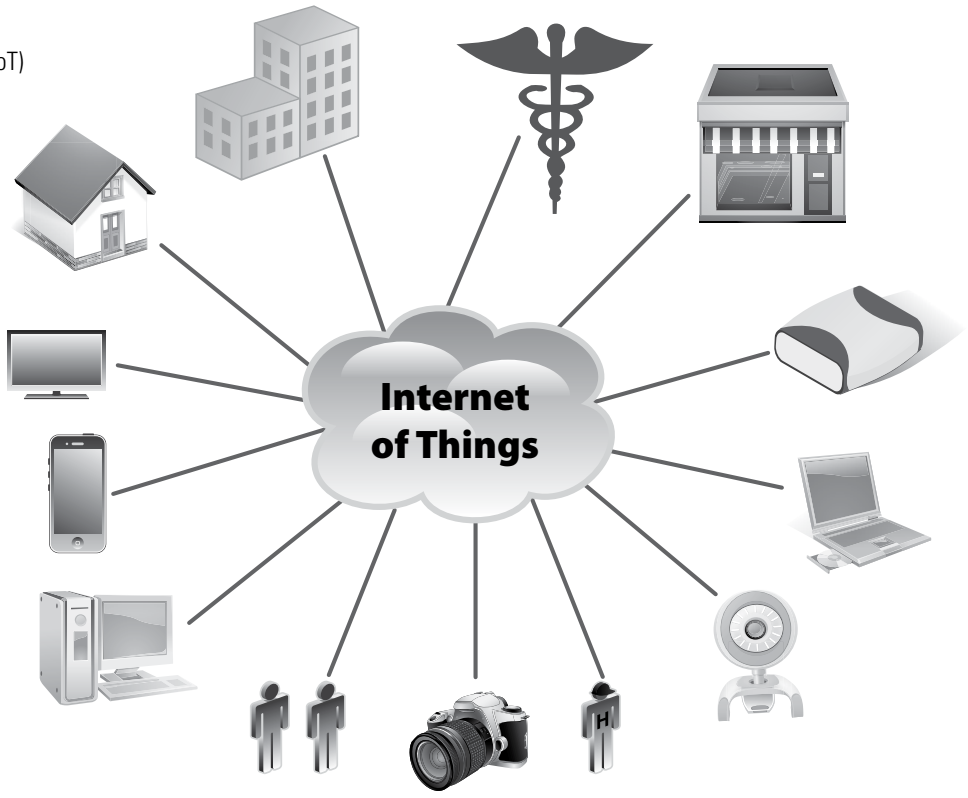


FIGURE 1-3
Internet of Things (IoT) supports any-to-any connectivity.

stay connected no matter where you are and what devices you need to connect. FIGURE 1-3 shows how the IoT is making the world a digitally connected one. The IoT magnifies the risk, threat, and vulnerability issues, given that a hacker or attacker can gain unauthorized access to any IP-connected device. Once access to an IP-connected device is granted, data can be stolen or damage can be done if the attacker desires. It's this "dark villain" nature of a hacker that helped label hackers as "black hats."

Internet growth has also been driven by generational differences. **Generation Y**'s culture is taking over as baby boomers begin to retire. This new generation grew up with cell phones, **smartphones**, and "always-on" Internet access. These devices provide real-time communication. Today's personal communications include Voice over IP (VoIP), text messaging, instant messaging (IM), and chatting as well as audio and video conferencing. These real-time, Session Initiation Protocol-enabled (SIP-enabled) applications are commonly known as **unified communications**. Examples of unified communication applications include Google Chat™ instant messaging service, Yahoo!® Messenger, WebEx,™ GoToMeeting,™ and Skype™ for Business's online meeting features.

Meanwhile, an **information security** war is raging. The battlefield is cyberspace and the enemies are already within the gates. To make matters worse, the enemy is everywhere—both in the local area and around the world. The enemy seeks your sensitive data. Thus, the name of the game for an attacker is to gain unauthorized access. **Unauthorized access** means that the attacker obtains your authorized logon ID and password without your permission.

Using those logon credentials, the attacker gains access to the same systems and applications that your access permits. If unauthorized access is granted, then depending on that user's access controls, sensitive data may be accessible and can be downloaded. For this reason, information technology infrastructures need proper security controls. This information security war has created a great demand for information systems security and information assurance professionals—for a new kind of cyberwarrior to help defend security and business interests.

Risks, Threats, and Vulnerabilities

This book introduces the dangers of cyberspace and discusses how to address those dangers. It explains how to identify and combat the dangers common in **information systems** and IT infrastructures. To understand how to make computers more secure, you first need to understand the concepts of risks, threats, and vulnerabilities.

Risk is the likelihood that something bad will happen to an asset. It is the level of exposure to some event that has an effect on an asset. In the context of IT security, an asset can be a computer, a database, or a piece of information. Examples of risk include the following:

- Losing data
- Losing business because a disaster has destroyed your building
- Failing to comply with laws and regulations

A **threat** is any action that could damage an asset. Information systems face both natural and human-induced threats. The threats of flood, earthquake, or severe storms require organizations to create plans to ensure that business operation continues and that the organization can recover. A **business continuity plan (BCP)** gives priorities to the functions an organization needs to keep going. **A disaster recovery plan (DRP)** defines how a business gets back on its feet after a major disaster such as a fire or hurricane. Human-caused threats to a computer system include viruses, malicious code, and unauthorized access. A **virus** is a computer program written to cause damage to a system, an application, or data. **Malicious code**, or **malware**, is a computer program written to cause a specific action to occur, such as erasing a hard drive. These threats can harm an individual, business, or organization.

A **vulnerability** is a weakness that allows a threat to be realized or to have an effect on an asset. To understand what a vulnerability is, think about lighting a fire. Lighting a fire is not necessarily bad. If you are cooking a meal on a grill, you will need to light a fire in the grill. The grill is designed to contain the fire and should pose no danger if used properly. On the other hand, lighting a fire in a computer data center will likely cause damage. A grill is not vulnerable to fire, but a computer data center is. A threat by itself does not always cause damage; there must be a *vulnerability* for a threat to be realized.

Vulnerabilities can often result in legal liabilities. Any vulnerability that allows a threat to be realized may result in legal action. Since computers must run software to be useful, and since humans write software, software programs inevitably contain errors. Thus, software vendors must protect themselves from the liabilities of their own vulnerabilities with an **End-User License Agreement (EULA)**. A EULA takes effect when the user opens the package and installs the software. All software vendors use EULAs. That means the burden of protecting IT systems and data lies on internal information systems security professionals.

End-User License Agreements (EULAs)

EULAs are license agreements between a user and a software vendor. EULAs protect the software vendor from claims arising from the behavior of imperfect software. EULAs typically contain a warranty disclaimer. This limits their liability from software bugs and weaknesses that hackers can exploit.

Here is an excerpt from Microsoft's EULA, stating that the company offers only "limited" warranties for its software. The EULA also advises that the software product is offered "as is and with all faults."

DISCLAIMER OF WARRANTIES. THE LIMITED WARRANTY THAT APPEARS ABOVE IS THE ONLY EXPRESS WARRANTY MADE TO YOU AND IS PROVIDED IN LIEU OF ANY OTHER EXPRESS WARRANTIES (IF ANY) CREATED BY ANY DOCUMENTATION OR PACKAGING. EXCEPT FOR THE LIMITED WARRANTY AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, MICROSOFT AND ITS SUPPLIERS PROVIDE THE SOFTWARE PRODUCT AND SUPPORT SERVICES (IF ANY) AS IS AND WITH ALL FAULTS, AND HEREBY DISCLAIM ALL OTHER WARRANTIES AND CONDITIONS....

Microsoft's EULA also limits its financial liability to the cost of the software or US$5, whichever is greater:

LIMITATION OF LIABILITY. ANY REMEDIES NOTWITHSTANDING ANY DAMAGES THAT YOU MIGHT INCUR FOR ANY REASON WHATSOEVER (INCLUDING, WITHOUT LIMITATION, ALL DAMAGES REFERENCED ABOVE AND ALL DIRECT OR GENERAL DAMAGES), THE ENTIRE LIABILITY OF MICROSOFT AND ANY OF ITS SUPPLIERS UNDER ANY PROVISION OF THIS EULA AND YOUR EXCLUSIVE REMEDY FOR ALL OF THE FOREGOING (EXCEPT FOR ANY REMEDY OF REPAIR OR REPLACEMENT ELECTED BY MICROSOFT WITH RESPECT TO ANY BREACH OF THE LIMITED WARRANTY) SHALL BE LIMITED TO THE GREATER OF THE AMOUNT ACTUALLY PAID BY YOU FOR THE SOFTWARE PRODUCT OR U.S.$5.00. THE FOREGOING LIMITATIONS, EXCLUSIONS AND DISCLAIMERS (INCLUDING SECTIONS 9, 10 AND 11 ABOVE) SHALL APPLY TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, EVEN IF ANY REMEDY FAILS ITS ESSENTIAL PURPOSE.

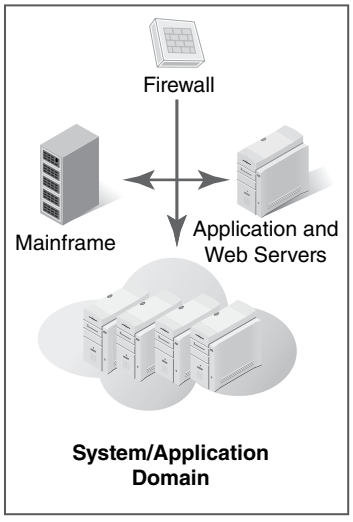
What Is Information Systems Security?

The term *security* is easiest to define by breaking it into pieces. An information system consists of the hardware, operating system, and application software that work together to collect, process, and store data for individuals and organizations. Thus **information systems security** is the collection of activities that protect the information system and the data stored in it. Many U.S. and international laws now require this kind of security assurance. Organizations must address this need head-on. **FIGURE 1-4** reviews the types of information commonly found within an IT infrastructure.

U.S. Compliance Laws Drive Need for Information Systems Security

Cyberspace brings new threats to people and organizations. People need to protect their privacy. Businesses and organizations are responsible for protecting both their intellectual property and any personal or private data they handle. Various laws require organizations to use security controls to protect private and confidential data. Recent U.S. laws related to information security include the following:

- **Federal Information Security Management Act (FISMA)**—Passed in 2002, FISMA requires federal civilian agencies to provide security controls over resources that support federal operations.



- Privacy Data of Individuals
  - Name, address, date of birth
  - Social Security number
  - Bank name, account number
  - Credit card account number
  - Utility account number
  - Mortgage account number
  - Insurance policy number
  - Securities and brokerage account numbers
- Corporate Intellectual Property
  - Trade secrets
  - Product development
  - Sales and marketing strategies
  - Financial records
  - Copyrights, patents, etc.
- Online B2C and B2B Transactions
  - Online banking
  - Online health care and insurance claims
  - E-commerce, e-government, services
  - Online education and transcripts
- Government Intellectual Property
  - National security
  - Military and DoD strategies

FIGURE 1-4
What are we securing?

- **Federal Information Security Modernization Act (FISMA)**—Passed in 2014, FISMA was enacted to update FISMA 2002 with information on modern threats as well as security controls and best practices.
- **Sarbanes-Oxley Act (SOX)**—Passed in 2002, SOX requires publicly traded companies to submit accurate and reliable financial reporting. This law does not require securing private information, but it does require security controls to protect the confidentiality and integrity of the reporting itself.
- **Gramm-Leach-Bliley Act (GLBA)**—Passed in 1999, GLBA requires all types of financial institutions to protect customers' private financial information.
- **Health Insurance Portability and Accountability Act (HIPAA)**—Passed in 1996, HIPAA requires health care organizations to have security and privacy controls implemented to ensure patient privacy.
- **Children's Internet Protection Act (CIPA)**—Passed in 2000 and updated in 2011, CIPA requires public schools and public libraries to use an Internet safety policy. The policy must address the following:
  - Restricting children's access to inappropriate matter on the Internet
  - Ensuring children's security when using email, chatrooms and other electronic communications
  - Restricting hacking and other unlawful activities by children online
  - Disclosing and distributing personal information about children without permission
  - Restricting children's access to harmful materials
  - Warning children on the use and dangers of social media

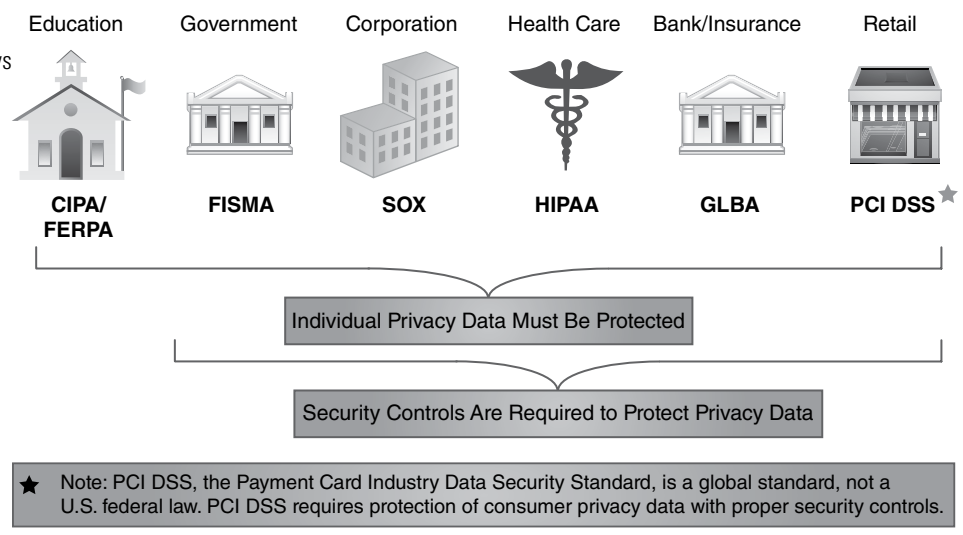


FIGURE 1-5
U.S. compliance laws drive the need for information systems security.

- **Family Educational Rights and Privacy Act (FERPA)**—Passed in 1974, FERPA protects the private data of students and their school records.

FIGURE 1-5 shows these laws by industry.

Tenets of Information Systems Security

Most people agree that private information should be secure. But what does "secure information" really mean? Information that is secure satisfies three main tenets, or properties, of information. If you can ensure these three tenets, you satisfy the requirements of secure information. The three tenets are as follows:

- **Confidentiality**—Only authorized users can view information.
- **Integrity**—Only authorized users can change information.
- **Availability**—Information is accessible by authorized users whenever they request the information.

FIGURE 1-6 illustrates the three tenets of information systems security. When you design and use security controls, you are addressing one or more of these tenets.

When finding solutions to security issues, you must use the C-I-A triad. You have to define your organization's security baseline goals using this triad for a typical IT infrastructure. Once defined, these goals will translate into security controls and requirements based on the type of data you are protecting.

Technical TIP

Some systems security professionals refer to the tenets as the A-I-C triad to avoid confusion with the U.S. Central Intelligence Agency, commonly known as the CIA.

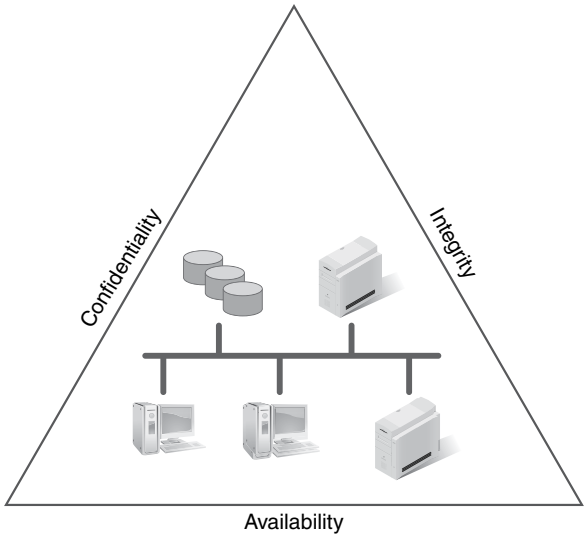


FIGURE 1-6
The three tenets of information systems security.

Identity Theft

Identity theft affects about 15 million U.S. citizens each year, with financial losses costing upward of $50 billion. Identity theft is a major threat to U.S. consumers. Many elements make up a person's identity. These include but are not limited to the following:

- Full name
- Mailing address
- Date of birth
- Social Security number
- Bank name
- Bank account number
- Credit card account number
- Utility account number
- Medical record number
- Mortgage account number
- Insurance policy number
- Securities and investment account numbers

For example, an impostor can access your accounts with just your name, home address, and Social Security number. Paper statements and account numbers tossed in the garbage can be retrieved by an unscrupulous person, making it easier for your privacy data and financial account information to be compromised. Shredding those documents before discarding them reduces the possibility of loss.

This threat extends beyond mere financial loss. Identity theft can damage your Fair Isaac Corp. (**FICO**) personal credit rating. This could stop you from getting a bank loan, mortgage, or credit card. It can take years to clean up your personal credit history. FICO is a publicly traded company that provides information used by Equifax, Experian, and TransUnion, the three largest consumer credit-reporting agencies in the United States.

Confidentiality

Confidentiality is a common term. It means guarding information from everyone except those with rights to it. Confidential information includes the following:

- Private data of individuals
- Intellectual property of businesses
- National security for countries and governments

U.S. compliance laws that protect citizens' private data require businesses and organizations to have proper security controls to ensure confidentiality.

With the growth in e-commerce, more people are making online purchases with credit cards. This requires people to enter private data into e-commerce websites. Consumers should be careful to protect their personal identity and private data. Laws require organizations to use security controls to protect customers' private data. A **security control** is something an organization does to help reduce risk. Examples of such controls include the following:

- Conducting annual security awareness training for employees. This helps remind staff about proper handling of private data. It also drives awareness of the organization's framework of security policies, standards, procedures, and guidelines.
- Putting an **IT security policy framework** in place. A policy framework is like an outline that identifies where security controls should be used.
- Designing a layered security solution for an IT infrastructure. The more layers or compartments that block or protect private data and intellectual property, the more difficult the data and property are to find and steal.
- Performing periodic security risk assessments, audits, and penetration tests on websites and IT infrastructure. This is how security professionals verify that they have properly installed the controls.
- Enabling security incident and event monitoring at your Internet entry and exit points. This is like using a microscope to see what is coming in and going out.
- Using automated workstation and server antivirus and malicious software protection. This is the way to keep viruses and malicious software out of your computer.
- Using more stringent access controls beyond a logon ID and password for sensitive systems, applications, and data. Logon IDs with passwords are only one check of the user. Access to more sensitive systems should have a second test to confirm the user's identity.
- Minimizing software weaknesses in your computers and servers by updating them with patches and security fixes. This is the way to keep your operating system and application software up to date.

Protecting private data is the process of ensuring data confidentiality. Organizations must use proper security controls specific to this concern. Some examples include the following:

- Defining organization-wide policies, standards, procedures, and guidelines to protect confidential data. These are instructions for how to handle private data.
- Adopting a **data classification standard** that defines how to treat data throughout your IT infrastructure. This is the road map for identifying what controls are needed to keep data safe.
- Limiting access to systems and applications that house confidential data to only those authorized to use that data.

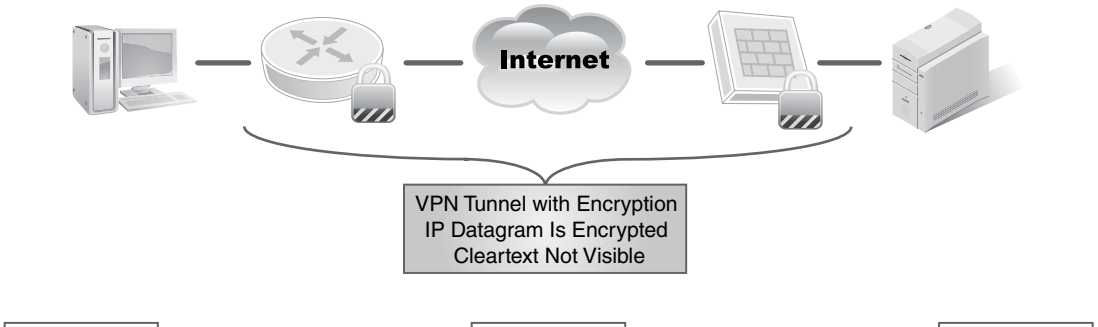


FIGURE 1-7
Encryption of cleartext into ciphertext.

- Using cryptography techniques to hide confidential data and keep that data invisible to unauthorized users.
- Encrypting data that cross the public Internet.
- Encrypting data that are stored within databases and storage devices.

Sending data to other computers using a network means you have to take special steps to keep confidential data from unauthorized users. **Cryptography** is the practice of hiding data and keeping it away from unauthorized users. **Encryption** is the process of transforming data from cleartext into **ciphertext**. Cleartext data are data that anyone can read. Ciphertext is the scrambled data that are the result of encrypting cleartext. An example of this process is shown in **FIGURE 1-7**.

Data privacy is so important that local and state governments are starting to pass laws to protect it by extending federal laws.

Integrity

Integrity deals with the validity and accuracy of data. Data lacking integrity—that is, data that are not accurate or not valid—are of no use. For some organizations, data and information are intellectual property assets. Examples include copyrights, patents, secret formulas, and customer databases. This information can have great value. Unauthorized changes can undermine the data's value. This is why integrity is a tenet of systems security. **FIGURE 1-8** shows what is meant by data integrity and whether that data are usable. Sabotage and corruption of data integrity are serious threats to an organization, especially if the data are critical to business operations.

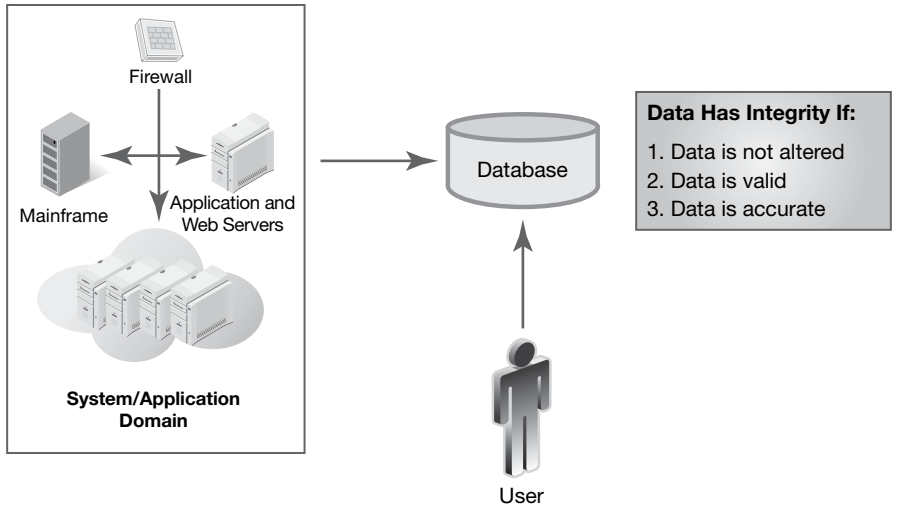
Availability

Availability is a common term in everyday life. For example, you probably pay attention to the availability of your Internet service, TV service, or cell phone service. In the context of information security, availability is generally expressed as the amount of time users can

⚠ WARNING

Never enter private data in an email in cleartext. Remember, email traffic transmits through the Internet in cleartext. This means your data are completely visible to whomever sees the email. Also, never enter private data in a website if that site is not a trusted host that can be checked by telephone or other means. Never enter private data into a website or web application that does not use encryption (e.g., look for the lock icon in your browser to verify if **Hypertext Transfer Protocol Secure (HTTPS)** encryption is enabled on that website or application).

FIGURE 1-8
Data integrity.



use a system, application, and data. Common availability time measurements include the following:

- **Uptime**—Uptime is the total amount of time that a system, application, and data are accessible. Uptime is typically measured in units of seconds, minutes, and hours within a given calendar month. Often uptime is expressed as a percentage of time available, e.g., 99.5 percent uptime.
- **Downtime**—Downtime is the total amount of time that a system, application, and data are not accessible. Downtime also is measured in units of seconds, minutes, and hours for a calendar month.
- **Availability**—Availability is a mathematical calculation where A = (Total Uptime) / (Total Uptime + Total Downtime).
- **Mean time to failure (MTTF)**—MTTF is the average amount of time between failures for a particular system. Semiconductors and electronics do not break and have an MTTF of many years (25 or more years, etc.). Physical parts such as connectors, cabling, fans, and power supplies have a much lower MTTF (five years or less), given that wear and tear can break them.
- **Mean time to repair (MTTR)**—MTTR is the average amount of time it takes to repair a system, application, or component. The goal is to bring the system back up quickly.
- **Mean time between failures (MTBF)—**MTBF is the predicted amount of time between failures of an IT system during operation.
- **Recovery time objective (RTO)**—RTO is the amount of time it takes to recover and make a system, application, and data available for use after an outage. Business continuity plans typically define an RTO for mission-critical systems, applications, and data access.

How to Calculate Monthly Availability

For a given 30-day calendar month, the total amount of uptime equals:

30 days × 24 hours/day × 60 minutes/hour = 43,200 minutes

For a 28-day calendar month (February), the total amount of uptime equals:

28 days × 24 hours/day × 60 minutes/hour = 40,320 minutes

Using the formula

Availability = (Total Uptime) / (Total Uptime + Total Downtime)

calculate the availability factor for a 30-day calendar month with 30 minutes of scheduled downtime in that calendar month as:

Availability = (43,200 minutes) / (43,200 minutes + 30 minutes) = 0.9993, or 99.93%

Telecommunications and Internet service providers offer their customers **service-level agreements (SLAs)**. An SLA is a contract that guarantees a minimum monthly availability of service for wide area network (WAN) and Internet access links. SLAs accompany WAN services and dedicated Internet access links. Availability measures a monthly uptime service-level commitment. As in the monthly availability example discussed in the sidebar, 30 minutes of downtime in a 30-day calendar month equates to 99.993 percent availability. Service providers typically offer SLAs ranging from 99.5 percent to 99.999 percent availability.

The Seven Domains of a Typical IT Infrastructure

What role do the three tenets of systems security play in a typical IT infrastructure? First, let's review what a typical IT infrastructure looks like. Whether in a small business, large government body, or publicly traded corporation, most IT infrastructures consist of the seven domains shown in **FIGURE 1-9**: User, Workstation, LAN, LAN-to-WAN, WAN, Remote Access, and System/Application Domains.

A typical IT infrastructure usually has these seven domains. Each one requires proper security controls. These controls must meet the requirements of the C-I-A triad. The following is an overview of the seven domains and the risks, threats, and vulnerabilities you will commonly find in today's IT environments.

User Domain

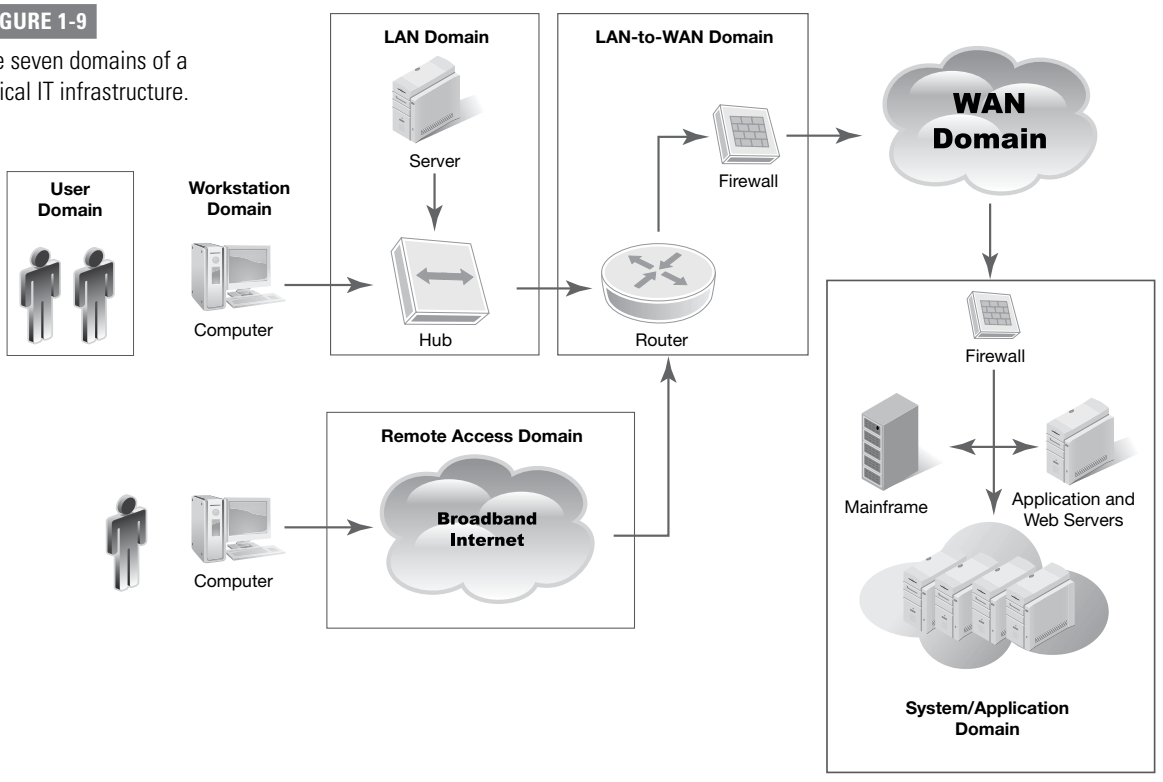
The User Domain defines the people who access an organization's information system.

User Domain Roles, Responsibilities, and Accountability

Here's an overview of what should go on in the User Domain:

- **Roles and tasks**—Users can access systems, applications, and data depending upon their defined access rights. Employees must conform to the staff manual and policies.

FIGURE 1-9
The seven domains of a typical IT infrastructure.



The User Domain is where you will find an **acceptable use policy (AUP)**. An AUP defines what users are allowed and not allowed to do with organization-owned IT assets. It's like a rule book that employees must follow. Violation of these rules can be grounds for dismissal. This is where the first layer of defense starts for a layered security strategy.

- **Responsibilities**—Employees are responsible for their use of IT assets. New legislation means that for most organizations it's a best practice to introduce an AUP. Organizations may require staff, contractors, or other third parties to sign an agreement to keep information confidential. Some require a criminal background check for sensitive positions. The department manager or human resources manager is usually in charge of making sure employees sign and follow an AUP.
- **Accountability**—Typically, an organization's human resources department is accountable for implementing proper employee background checks. These should be performed for individuals who will be accessing sensitive data.

Risks, Threats, and Vulnerabilities Commonly Found in the User Domain

The User Domain is the weakest link in an IT infrastructure. Anyone responsible for computer security must understand what motivates someone to compromise an organization's system, applications, or data. TABLE 1-2 lists the risks and threats commonly found in the User Domain as well as plans you can use to prevent them.

TABLE 1-2 Risks, threats, vulnerabilities, and mitigation plans for the User Domain.

RISK, THREAT, OR VULNERABILITY	MITIGATION
Unauthorized access	Users must be made aware of phishing emails, pretexting or cons, keyboard loggers, and perpetrators impersonating an IT or delivery person in an attempt to obtain logon ID and password credentials.
Lack of user awareness	Conduct security awareness training, display security awareness posters, insert reminders in banner greetings, and send email reminders to employees.
User apathy toward policies	Conduct annual security awareness training, implement acceptable use policy, update staff manual and handbook, discuss during performance reviews.
Security policy violations	Place employee on probation, review AUP and employee manual, discuss during performance reviews.
User insertion of CDs and USB drives with personal photos, music, and videos	Disable internal CD drives and USB ports. Enable automatic antivirus scans for inserted media drives, files, and email attachments. An antivirus scanning system examines all new files on your computer's hard drive for viruses. Set up antivirus scanning for emails with attachments.
User downloads of photos, music, and videos	Enable **content filtering** and antivirus scanning for email attachments. Content-filtering network devices are configured to permit or deny specific domain names in accordance with AUP definitions.
User destruction of systems, applications, or data	Restrict users' access to only those systems, applications, and data needed to perform their jobs. Minimize write/delete permissions to the data owner only.
Attacks on the organization or acts of sabotage by disgruntled employees	Track and monitor abnormal employee behavior, erratic job performance, and use of IT infrastructure during off-hours. Begin IT access control lockout procedures based on AUP monitoring and compliance.
Employee romance gone bad	Track and monitor abnormal employee behavior and use of IT infrastructure during off-hours. Begin IT access control lockout procedures based on AUP monitoring and compliance.
Employee blackmail or extortion	Track and monitor abnormal employee behavior and use of IT infrastructure during off-hours. Enable intrusion detection system/intrusion prevention system (IDS/IPS) monitoring for sensitive employee positions and access. IDS/IPS security appliances examine the IP data streams for inbound and outbound traffic. Alarms and alerts programmed within an IDS/IPS help identify abnormal traffic and can block IP traffic as per policy definition.

Workstation Domain

A **workstation** can be a desktop computer, a laptop computer, a special-purpose terminal, or any other device that connects to your network. Workstation computers are generally thin clients or thick clients. A **thin client** is software or an actual computer with no hard drive that runs on a network and relies on a server to provide applications, data, and all processing. Thin clients are commonly used in large organizations, libraries, and schools. In contrast, a **thick client** is more fully featured hardware that contains a hard drive and applications and processes data locally, going to the server mainly for file storage. An ordinary PC is an example of a thick client. Other devices that can be considered workstations are **personal digital assistants (PDAs)**, smartphones, and tablet PCs. You can find more details about mobile devices in the "Remote Access Domain" section.

Workstation Domain Roles, Responsibilities, and Accountability

Here's an overview of what should go on in the Workstation Domain:

- **Roles and tasks**—An organization's staff should have the access necessary to be productive. Tasks include configuring hardware, hardening systems, and verifying antivirus files. **Hardening** a system is the process of ensuring that controls are in place to handle any known threats. Hardening activities include ensuring that all computers have the latest software revisions, security patches, and system configurations. The Workstation Domain also needs additional layers of defense, a tactic referred to as **defense in depth**. Another common defense layer is implementing workstation logon IDs and passwords to protect this entry into the IT infrastructure.
- **Responsibilities**—An organization's desktop support group is responsible for the Workstation Domain. Enforcing defined standards is critical to ensuring the integrity of user workstations and data. The IT security personnel must safeguard controls within the Workstation Domain. Typically, human resources departments define proper access controls for workers based on their jobs. IT security personnel then assign access rights to systems, applications, and data based on this definition.
- **Accountability**—An organization's IT desktop manager is typically accountable for allowing employees the greatest use of the Workstation Domain. The director of IT security is generally in charge of ensuring that the Workstation Domain conforms to policy.

Risks, Threats, and Vulnerabilities Commonly Found in the Workstation Domain

The Workstation Domain requires tight security and access controls. This is where users first access systems, applications, and data. The Workstation Domain requires a logon ID and password for access. TABLE 1-3 lists the risks, threats, and vulnerabilities commonly found in the Workstation Domain, along with ways to protect against them.

LAN Domain

A **local area network (LAN)** is a collection of computers connected to one another or to a common connection medium. Network connection mediums can include wires, fiber-optic cables, or radio waves. LANs are generally organized by function or department. Once

TABLE 1-3 Risks, threats, vulnerabilities, and mitigation plans for the Workstation Domain.

RISK, THREAT, OR VULNERABILITY	MITIGATION
Unauthorized access to workstation	Enable password protection on workstations for access. Enable auto screen lockout for inactive times. Disable system admin rights for users.
Unauthorized access to systems, applications, and data	Define strict access control policies, standards, procedures, and guidelines. Implement a second level or layer of authentication to applications that contain sensitive data (e.g., **two-step authentication**).
Desktop or laptop computer operating system software vulnerabilities	Define a workstation operating system **vulnerability window** policy and standard. The vulnerability window is the gap in time a workstation is exposed to a known vulnerability until patched. Perform frequent **vulnerability assessment** scans as part of ongoing security operations.
Desktop or laptop application software vulnerabilities and software patch updates	Define a workstation application **software vulnerability** window policy. Update application software and security patches according to defined policies, standards, procedures, and guidelines.
Infection of a user's workstation or laptop computer by viruses, malicious code, or malware	Use workstation antivirus and malicious code policies, standards, procedures, and guidelines. Enable an automated antivirus protection solution that scans and updates individual workstations with proper protection.
User insertion of CDs, digital video discs (DVDs), or universal serial bus (USB) thumb drives into the organization's computers	Deactivate all CD, DVD, and USB ports. Enable automatic antivirus scans for inserted CDs, DVDs, and USB thumb drives that have files.
User downloads of photos, music, or videos via the Internet	Use content filtering and antivirus scanning at Internet entry and exit. Enable workstation auto-scans for all new files and automatic file quarantine for unknown file types.
User violation of AUP, which creates security risk for the organization's IT infrastructure	Mandate annual security awareness training for all employees. Set up security awareness campaigns and programs throughout the year.
Employees and users want to use their own smartphone or tablets, driving the need to support Bring Your Own Device (BYOD)	Develop a BYOD policy and procedure that allows employees to use their personal smartphones or mobile devices. BYOD policies and procedures typically permit the organization to data-wipe the user's smartphone or mobile device if it is lost or the employee is terminated.

connected, your computer can access systems, applications, possibly the Internet, and data. The third component in the IT infrastructure is the LAN Domain.

The physical part of the LAN Domain consists of the following:

- **Network interface card (NIC)**—The interface between the computer and the LAN physical media. The NIC has a 6-byte Media Access Control (MAC) layer address that serves as the NIC's unique hardware identifier.
- **Ethernet LAN**—This is a LAN solution based on the **IEEE 802.3 CSMA/CD** standard for 10/100/1,000Mbps Ethernet networking. **Ethernet** is the most popular LAN standard. Today's LAN standard is the **Institute of Electrical and Electronics Engineers (IEEE)** 802.3 **Carrier Sense Multiple Access/Collision Detection (CSMA/CD)** specification. Ethernet is available in 10-Mbps, 100-Mbps, 1-Gbps, 10-Gbps, 40-Gbps, and now 100-Gbps speeds for campus and metro Ethernet backbone connections.
- **Unshielded twisted-pair cabling**—This is the workstation cabling that uses RJ-45 connectors and jacks to physically connect to a 100Mbps/1Gbps/10Gbps Ethernet LAN switch. Today, organizations use Category 5 or Category 6 UTP transmission media to support high-speed data communications.
- **LAN switch**—This is the device that connects workstations into a physical Ethernet LAN. A switch provides dedicated Ethernet LAN connectivity for workstations and servers, providing maximum throughput and performance for each workstation. There are two kinds of LAN switch. A **Layer 2 switch** examines the MAC layer address and makes forwarding decisions based on MAC layer address tables. A **Layer 3 switch** examines the network layer address and routes packets based on routing protocol path determination decisions. A Layer 3 switch is the same thing as a router.
- **File server and print server**—These are high-powered computers that provide file sharing and data storage for users within a department. Print servers support shared printer use within a department.
- **Wireless access point (WAP)**—For **wireless LANs (WLANs)**, radio transceivers are used to transmit IP packets from a WLAN NIC to a **wireless access point (WAP)**. The WAP transmits WLAN signals for mobile laptops to connect. The WAP connects back to the LAN switch using unshielded twisted-pair cabling.

Ethernet switches typically provide 100-Mbps or 1-Gbps connectivity for each workstation. Today, Ethernet LAN switches support 100-Mbps and 1-GigE desktop speeds and backbone connections at 10-Gbps and 40-Gpbs speeds. These backbone connections commonly use fiber-optic cabling.

The logical part of the LAN Domain consists of the following:

- **System administration**—Setup of user LAN accounts with logon ID and password access controls (that is, user logon information).
- **Design of directory and file services**—The servers, directories, and folders to which the user can gain access.
- **Configuration of workstation and server TCP/IP software and communication protocols**—This involves IP addressing, the **IP default gateway router**, **subnet mask address**, etc. The IP default gateway router acts as the entry/exit to the LAN. The subnet mask address defines the IP network number and IP host number.

- **Design of server disk storage space; backup and recovery of user data**—Provision for user data files on LAN disk storage areas where data are backed up and archived daily. In the event of data loss or corruption, data files can be recovered from the backed-up files.
- **Design of virtual LANs (VLANs)**—With Layer 2 and Layer 3 LAN switches, Ethernet ports can be configured to be on the same VLAN, even though they may be connected to different physically connected LANs. This is the same thing as configuring workstations and servers to be on the same Ethernet LAN or broadcast domain.

Users get access to their department's LAN and other applications according to what their job requires.

LAN Domain Roles, Responsibilities, and Accountability

Here's an overview of what should go on in the LAN Domain:

- **Roles and tasks**—The LAN Domain includes both physical network components and logical configuration of services for users. Management of the physical components includes:
  - Cabling
  - NICs
  - LAN switches
  - Wireless access points (WAPs)

  LAN system administration includes maintaining the master lists of user accounts and access rights. In the LAN Domain, two-step authentication might be required. Two-step authentication is like a gate whereby the user must confirm his or her identity a second time. This mitigates the risk of unauthorized physical access.
- **Responsibilities**—The LAN support group is in charge of the LAN Domain. This includes both the physical component and logical elements. LAN system administrators must maintain and support departments' file and print services and configure access controls for users.
- **Accountability**—The LAN manager's duty is to maximize use and integrity of data within the LAN Domain. Typically, the director of IT security must ensure that the LAN Domain conforms to policy.

Risks, Threats, and Vulnerabilities Commonly Found in the LAN Domain

The LAN Domain also needs strong security and access controls. Users can access company-wide systems, applications, and data from the LAN Domain. This is where the third layer of defense is required. This defense protects the IT infrastructure and the LAN Domain. TABLE 1-4 lists the risks, threats, and vulnerabilities commonly found in the LAN Domain, along with appropriate risk-reducing strategies.

LAN-to-WAN Domain

The LAN-to-WAN Domain is where the IT infrastructure links to a wide area network and the Internet. Unfortunately, connecting to the Internet is like rolling out the red carpet for bad guys. The Internet is open, public, and easily accessible by anyone. Most Internet traffic

TABLE 1-4 Risks, threats, vulnerabilities, and mitigation plans for the LAN Domain.

RISK, THREAT, OR VULNERABILITY	MITIGATION
Unauthorized access to LAN	Make sure wiring closets, data centers, and computer rooms are secure. Do not allow anyone access without proper ID.
Unauthorized access to systems, applications, and data	Define strict access control policies, standards, procedures, and guidelines. Implement a second-level identity check to gain access to sensitive systems, applications, and data. Restrict users from access to LAN folders and read/write/delete privileges on specific documents as needed.
LAN server operating system software vulnerabilities	Define server/desktop/laptop vulnerability window policies, standards, procedures, and guidelines. Conduct periodic LAN Domain vulnerability assessments to find software gaps. A vulnerability assessment is a software review that identifies bugs or errors in software. These bugs and errors go away when you upload software patches and fixes.
LAN server application software vulnerabilities and software patch updates	Define a strict software vulnerability window policy requiring quick software patching.
Unauthorized access by rogue users on WLANs	Use WLAN **network keys** that require a password for wireless access. Turn off broadcasting on WAPs. Require second-level authentication prior to granting WLAN access.
Compromised confidentiality of data transmissions via WLAN	Implement encryption between workstation and WAP to maintain confidentiality.
LAN servers with different hardware, operating systems, and software make them difficult to manage and troubleshoot	Implement LAN server and configuration standards, procedures, and guidelines.

is cleartext. That means it's visible and not private. Network applications use two common transport protocols: Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). Both TCP and UDP use port numbers to identify the application or function; these port numbers function like channels on a TV, dictating which station you're watching. When a packet is sent via TCP or UDP, its port number appears in the packet header. Because many services are associated with a common port number, knowing the port number essentially reveals what type of packet it is. This is like advertising to the world what you are transmitting.

Examples of common TCP and UDP port numbers include the following:

- **Port 80: Hypertext Transfer Protocol (HTTP)**—HTTP is the communications protocol between web browsers and websites with data in cleartext.
- **Port 20: File Transfer Protocol (FTP)**—FTP is a protocol for performing file transfers. FTP uses TCP as a connection-oriented data transmission but in cleartext, including

the password. *Connection-oriented* means individual packets are numbered and acknowledged as being received, to increase integrity of the file transfer.

- **Port 69: Trivial File Transfer Protocol (TFTP)**—TFTP is a protocol for performing file transfers. TFTP utilizes UDP as a connectionless data transmission but in cleartext. This is used for small and quick file transfers, given that it does not guarantee individual packet delivery.
- **Port 23: Terminal Network (Telnet)**—**Telnet** is a network protocol for performing remote terminal access to another device. Telnet uses TCP and sends data in cleartext.
- **Port 22: Secure Shell (SSH)**—SSH is a network protocol for performing remote terminal access to another device. SSH encrypts the data transmission for maintaining confidentiality of communications.

A complete list of well-known port numbers from 0 to 1023 is maintained by the Internet Assigned Numbers Authority (IANA). The IANA helps coordinate global domain name services, IP addressing, and other resources. Well-known port numbers are on the IANA website at *www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml.*

Because the TCP/IP suite of protocols lacks security, the need is greater for security controls in dealing with protocols in this family. The LAN-to-WAN Domain represents the fourth layer of defense for a typical IT infrastructure.

LAN-to-WAN Domain Roles, Responsibilities, and Accountability

Here's an overview of what should go on in the LAN-to-WAN Domain:

- **Roles and tasks**—The LAN-to-WAN Domain includes both the physical pieces and logical design of security appliances. It is one of the most complex areas to secure within an IT infrastructure. You need to maintain security while giving users as much access as possible. Physical parts need to be managed to give easy access to the service. The security appliances must be logically configured to adhere to policy definitions.

  This will get the most out of availability, ensure data integrity, and maintain confidentiality. The roles and tasks required within the LAN-to-WAN Domain include managing and configuring the following:

  - **IP routers**—An IP router is a network device used to transport IP packets to and from the Internet or WAN. Path determination decisions forward IP packets. Configuration tasks include IP routing and access control lists (ACLs). Like a filter, ACLs are used to permit and deny traffic.
  - **IP stateful firewalls**—An **IP stateful firewall** is a security appliance used to filter inbound IP packets based on various ACL definitions configured for IP, TCP, and UDP packet headers. A stateful firewall can examine IP, TCP, or UDP packet headers for filtering.
  - **Demilitarized zone (DMZ)**—The DMZ is a LAN segment in the LAN-to-WAN Domain that acts as a buffer zone for inbound and outbound IP traffic. External servers such as web servers, **proxy servers**, and email servers can be placed here for greater isolation and screening of IP traffic.
  - **Intrusion detection system (IDS)**—An IDS security appliance examines IP data streams for common attack and malicious intent patterns. IDSs are passive, going only so far as to trigger an alarm, but they will not actively block traffic.

- **Intrusion prevention system (IPS)**—An IPS does the same thing as an IDS but can block IP data streams identified as malicious. IPSs can end the actual communication session, filter by source IP addresses, and block access to the targeted host.
- **Proxy servers**—A proxy server acts as a middleman between a workstation and the external target. Traffic goes to the intermediary server that is acting as the proxy. Data can be analyzed and properly screened before they are relayed into the IT infrastructure by what are called **proxy firewalls** or **application gateway firewalls**.
- **Web content filter**—This security appliance can prevent content from entering an IT infrastructure based on filtering of domain names or of keywords within domain names.
- **Email content filter and quarantine system**—This security appliance can block content within emails or unknown file attachments for proper antivirus screening and quarantining. Upon review, the email and attachments can be forwarded to the user.

- **Security information and event management (SIEM)**—This includes monitoring the IT assets within the LAN-to-WAN Domain, including the DMZ VLAN, firewalls, IDS/IPS, and other security appliances to maximize confidentiality, integrity, and availability and monitor for security incidents and alarms triggered by specific events.
- **Responsibilities**—The network security group is responsible for the LAN-to-WAN Domain. This includes both the physical components and logical elements. Group members are responsible for applying the defined security controls.
- **Accountability**—Your organization's WAN network manager has a duty to manage the LAN-to-WAN Domain. Typically, the director of IT security ensures that the LAN-to-WAN Domain security policies, standards, procedures, and guidelines are used.

Risks, Threats, and Vulnerabilities Commonly Found in the LAN-to-WAN Domain

The LAN-to-WAN Domain requires strict security controls, given the risks and threats of connecting to the Internet. This domain is where all data travel into and out of the IT infrastructure. The LAN-to-WAN Domain provides Internet access for the entire organization and acts as the entry and exit point for the WAN. This is also known as the Internet ingress/egress point. The LAN-to-WAN Domain is where the fourth layer of defense is required. **TABLE 1-5** lists the risks, threats, and vulnerabilities commonly found in the LAN-to-WAN Domain, along with appropriate risk-reduction strategies.

WAN Domain

The Wide Area Network (WAN) Domain connects remote locations. As network costs drop, organizations can afford faster Internet and WAN connections. Today, telecommunications service providers sell the following:

- **Nationwide optical backbones**—Optical backbone trunks for private optical backbone networks.
- **End-to-end IP transport**—IP services and connectivity using the service provider's IP networking infrastructure.

TABLE 1-5 Risks, threats, vulnerabilities, and mitigation plans for the LAN-to-WAN Domain.

RISK, THREAT, OR VULNERABILITY	MITIGATION
Unauthorized network probing and port scanning	Disable **ping**, probing, and port scanning on all exterior IP devices within the LAN-to-WAN Domain. Ping uses the Internet Control Message Protocol (ICMP) echo-request and echo-reply protocol. Disallow IP port numbers used for probing and scanning and monitor with IDS/IPS.
Unauthorized access through the LAN-to-WAN Domain	Apply strict security monitoring controls for intrusion detection and prevention. Monitor for inbound IP traffic anomalies and malicious-intent traffic. Block traffic right away if malicious.
Denial of service (DoS)/distributed denial of service (DDoS) attacks on external public-facing IP's and Internet link	Upstream Internet service providers (ISPs) must participate in DoS/DDoS attack prevention and discarding of IP packets when a stream of half-open TCP SYN packets start to flood the ISP link.
IP router, firewall, and network appliance operating system software vulnerability	Define a strict zero-day vulnerability window definition. Update devices with security fixes and software patches right away.
IP router, firewall, and network appliance configuration file errors or weaknesses	Conduct postconfiguration penetration tests of the layered security solution within the LAN-to-WAN Domain. Test inbound and outbound traffic and fix any gaps.
The ability for remote users to access the organization's infrastructure and download sensitive data	Apply and enforce the organization's data classification standard. Deny outbound traffic using source IP addresses in access control lists. If remote downloading is allowed, encrypt where necessary.
Download of unknown file type attachments from unknown sources	Apply file transfer monitoring, scanning, and alarming for unknown file types from unknown sources.
Unknown email attachments and embedded URL links received by local users	Apply email server and attachment antivirus and email quarantining for unknown file types. Stop domain-name website access based on content-filtering policies.
Lost productivity due to local users surfing the Web and not focusing on work tasks	Apply domain-name content filtering at the Internet entry/access point.

- **Multisite WAN cloud services**—IP services and connectivity offered for multisite services such as **Multiprotocol Label Switching (MPLS)** WAN services. MPLS uses labels or tags to make virtual connections between endpoints in a WAN.
- **Metropolitan Ethernet LAN connectivity**—Ethernet LAN connectivity offered within a city's area network.
- **Dedicated Internet access**—A broadband Internet communication link usually shared within an organization.

- **Managed services**—Router management and security appliance management $24 \times 7 \times 365$.
- **Service-level agreements (SLAs)**—Contractual commitments for monthly service offerings such as availability, packet loss, and response time to fix problems.

The WAN Domain represents the fifth layer of security for an overall IT infrastructure. WAN services can include dedicated Internet access and managed services for customers' routers and firewalls. Management agreements for availability and response times to outages are common. Networks, routers, and equipment require continuous monitoring and management to keep WAN service available.

WAN Domain Roles, Responsibilities, and Accountability

Here's an overview of what should go on in the WAN Domain:

- **Roles and tasks**—The WAN Domain includes both physical components and the logical design of routers and communication equipment. It is the second most complex area to secure within an IT infrastructure. Your goal is to allow users the most access possible while making sure what goes in and out is safe. The roles and tasks required within the WAN Domain include managing and configuring the following:
  - **WAN communication links**—These are the physical communication links provided as a digital or optical service terminated at your facility. Broadband connection speeds can range among the following:
    - DS0 (64 Kbps) to DS1 (1.544 Mbps) to DS3 (45 Mbps) for digital service
    - OC-3 (155 Mbps) to OC-12 (622 Mbps) to OC-48 (2,488 Mbps) for optical service
    - 10/100/1000 Mbps Metro Ethernet LAN connectivity, depending on physical distance
  - **IP network design**—This is the logical design of the IP network and addressing schema. This requires network engineering, design of alternate paths, and selection of IP routing protocol.
  - **IP stateful firewall**—This is a security appliance that is used to filter IP packets and block unwanted IP, TCP, and UDP packet types from entering or leaving the network. Firewalls can be installed on workstations or routers or as standalone devices protecting LAN segments.
  - **IP router configuration**—This is the actual router configuration information for the WAN backbone and edge routers used for IP connections to remote locations. The configuration must be based on the IP network design and addressing schema.
  - **Virtual private networks (VPNs)**—A VPN is a dedicated encrypted tunnel from one endpoint to another. The VPN tunnel can be created between a remote workstation using the public Internet and a VPN router or a secure browser and a **Secure Sockets Layer virtual private network (SSL-VPN)** website.
  - **Multiprotocol Label Switching (MPLS)**—MPLS is a WAN software feature that allows customers to maximize performance. MPLS labels IP packets for rapid transport through virtual tunnels between designated endpoints. This is a form of Layer 1/Layer 3 overlay network and bypasses the routing function's path determination process once a long-lived flow is configured or dynamically determined.

  - **Simple Network Management Protocol (SNMP) network monitoring and management**—SNMP is used for network device monitoring, alarm, and performance.
  - **Router and equipment maintenance**—A requirement to perform hardware and firmware updates, upload new operating system software, and configure routers and filters.
- **Responsibilities**—The network engineer or WAN group is responsible for the WAN Domain. This includes both the physical components and logical elements. Network engineers and security practitioners set up the defined security controls according to defined policies. Note that because of the complexities of IP network engineering, many groups now outsource management of their WAN and routers to service providers. This service includes SLAs that ensure that the system is available and that problems are solved quickly. In the event of a WAN connection outage, customers call a toll-free number for their service provider's **network operations center (NOC)**.
- **Accountability**—Your organization's IT network manager must maintain, update, and provide technical support for the WAN Domain. Typically, the director of IT security ensures that the company meets WAN Domain security policies, standards, procedures, and guidelines.

Some organizations use the public Internet as their WAN infrastructure. Although it is cheaper, the Internet does not guarantee delivery or security.

Risks, Threats, and Vulnerabilities Commonly Found in the WAN Domain (Internet)

Telecommunication service providers are in the business of providing WAN connectivity for end-to-end communications. Service providers must take on the responsibility for securing their network infrastructure first. Customers who sign up for WAN communication services must review the terms, conditions, and limitations of liability within their service contract. This is important because organizations must figure out where their duties start and end regarding router management and security management.

The most critical aspect of a WAN services contract is how the service provider supplies troubleshooting, network management, and security management services. The WAN Domain is where the fifth layer of defense is required. **TABLE 1-6** lists the risks, threats, and vulnerabilities found in the Internet segment of the WAN Domain and appropriate risk-lowering strategies.

Telecommunications service providers sell WAN connectivity services. Some providers now also provide security management services. The following section presents WAN connectivity risks, threats, and vulnerabilities and risk-reducing strategies.

Risks, Threats, and Vulnerabilities Commonly Found in the WAN Domain (Connectivity)

Telecommunications companies are responsible for building and transporting customer IP traffic. Sometimes this IP traffic is bundled with dedicated Internet access, providing shared broadband access organization-wide. If organizations outsource their WAN infrastructure, management and security must extend to the service provider. Organizations must define security policies and needs for their managed security provider to put in place. **TABLE 1-7** lists the risks, threats, and vulnerabilities related to connectivity found in the WAN Domain and appropriate risk-lowering strategies.

TABLE 1-6 Risks, threats, vulnerabilities, and mitigation plans for the WAN Domain (Internet).

RISK, THREAT, OR VULNERABILITY	MITIGATION
Open, public, easily accessible to anyone who wants to connect	Apply acceptable-use policies in accord with the document "RFC 1087: Ethics and the Internet." Enact new laws regarding unauthorized access to systems, malicious attacks on IT infrastructures, and financial loss due to malicious outages.
Most Internet traffic sent in cleartext	Prohibit using the Internet for private communications without encryption and VPN tunnels. If you have a data classification standard, follow the policies, procedures, and guidelines specifically.
Vulnerable to eavesdropping	Use encryption and VPN tunnels for end-to-end secure IP communications. If you have a data classification standard, follow the policies, procedures, and guidelines.
Vulnerable to malicious attacks	Deploy layered LAN-to-WAN security countermeasures, DMZ with IP stateful firewalls, IDS/IPS for security monitoring, and quarantining of unknown email file attachments.
Vulnerable to DoS, DDoS, TCP SYN flooding, and IP spoofing attacks	Apply filters on exterior IP stateful firewalls and IP router WAN interfaces to block TCP SYN "open connections" and ICMP (echo-request) ping packets. Alert your Internet service provider (ISP) to put the proper filters on its IP router WAN interfaces in accordance with CERT Advisory CA-1996-21. This can be found here: *www.cert.org/advisories/CA-1996-21.html*.
Vulnerable to corruption of information and data	Encrypt IP data transmissions with VPNs. Back up and store data in offsite data vaults (online or physical data backup) with tested recovery procedures.
Inherently insecure TCP/IP applications (HTTP, FTP, TFTP, etc.)	Refer to your data classification standard for proper handling of data and use of TCP/IP applications. Never use TCP/IP applications for confidential data without proper encryption. Create a network management VLAN and isolate TFTP and SNMP traffic used for network management.
Email of **Trojans**, **worms**, and malicious software by hackers, attackers, and perpetrators	Scan all email attachments for type, antivirus, and malicious software at the LAN-to-WAN Domain. Isolate and quarantine unknown file attachments until further security review is conducted. Provide security awareness training to remind employees of dangers, such as embedded URL links and email attachments from unknown parties, and to urge them to be careful when clicking on links and opening files.

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. Global access makes it easy to connect to the Internet, email, and other business applications

TABLE 1-7 Risks, threats, vulnerabilities, and mitigation plans for the WAN Domain (connectivity).

RISK, THREAT, OR VULNERABILITY	MITIGATION
Commingling of WAN IP traffic on the same service provider router and infrastructure	Encrypt confidential data transmissions through service provider WAN using VPN tunnels.
Maintaining high WAN service availability	Obtain WAN service availability SLAs. Deploy redundant Internet and WAN connections when 100 percent availability is required.
Maximizing WAN performance and throughput	Apply WAN optimization and data compression solutions when accessing remote systems, applications, and data. Enable access control lists (ACLs) on outbound router WAN interfaces, in keeping with policy.
Using SNMP network management applications and protocols maliciously (ICMP, Telnet, SNMP, DNS, etc.)	Create separate WAN network management VLANs. Use strict firewall ACLs allowing SNMP manager and router IP addresses through the LAN-to-WAN Domain.
SNMP alarms and security monitoring 24 × 7 × 365	Outsource security operations and monitoring. Expand services to include managed security.

anywhere you can find a **Wireless Fidelity (Wi-Fi)** hotspot. The Remote Access Domain is important to have but dangerous to use. It introduces many risks and threats from the Internet.

Today's mobile worker depends on the following:

- **Highly available cell phone service**—Mobile workers need cell phone service to get in touch with office and support teams.
- **Real-time access for critical communications**—Use of text messaging or **instant messaging (IM) chat** on cell phones provides quick answers to short questions and does not require users to completely interrupt what they are doing.
- **Access to email from a mobile device**—Integration of email with cell phones, smartphones, tablets, PDAs, or **BlackBerry** devices provides users the ability to quickly respond to important email messages.
- **Broadband Wi-Fi Internet access**—Some nationwide service providers now offer Wi-Fi broadband access cards. They allow wireless access in major metro areas.
- **Local Wi-Fi hotspot**—Wi-Fi hotspots are abundant, including in airports, libraries, coffee shops, and retailers. Most are free, but some require that users pay for access.
- **Broadband Internet access to home office**—Staffers who work from home require broadband Internet access. This service is usually bundled with VoIP telephone and digital TV services.
- **Secure remote access to a company's IT infrastructure**—Remote workers require secure VPN tunnels to encrypt all IP data transmissions through the public Internet. This is critical if private data are being accessed remotely.

The scope of this domain is limited to remote access via the Internet and IP communications. The logical configuration of the Remote Access Domain requires IP network

engineering and VPN solutions. This section addresses individual remote access and large-scale remote access for many remote users. The Remote Access Domain represents the sixth layer of defense for a typical IT infrastructure.

Remote Access Domain Roles, Responsibilities, and Accountability

Here's an overview of what should go on in the Remote Access Domain:

- **Roles and tasks**—The Remote Access Domain connects mobile users to their IT systems through the public Internet. The mobile user must have a remote IP device able to connect to the Internet. Besides laptop computers, mobile users can use smartphones, tablets, and PDAs as handheld computers. The mobile software on these devices makes possible phone calls, voicemail, email, text messaging, and web browsing remotely.

The roles and tasks required within the Remote Access Domain include managing and designing the following:

- **Cell phones, smartphones, PDAs, and BlackBerry units**—Company-issued devices should be loaded with up-to-date firmware, operating system software, and patches according to defined policies. Policy should require use of passwords on this equipment.
- **Laptop VPN client software**—When organizations use VPN tunnels between the LAN-to-WAN Domain and remote-user laptop computers, you must select VPN software that meets your organization's specific needs and that works with your other software.
- **Secure browser software**—Webpages that use Hypertext Transfer Protocol Secure (HTTPS) need secure browsers. HTTPS encrypts the data transfer between secure browsers and secure webpages.

The Risk from Backdoor Analog Phone Lines and Modems

Some maintenance vendors use analog phone lines and modems to reach equipment. That means they do not use IP or SNMP protocols. Although this is convenient, it allows an insecure backdoor into the IT system. Attackers use tools that can get around an analog modem's password. Be alert for user workstations that are equipped with an analog modem connected to a backdoor analog phone line. Your company might not know that IT staff and software developers have set up these backdoors. This can be a risk because analog modems generally have few security controls.

The following are some of the best ways to reduce these risks and threats:

- Do not install single analog phone lines without going through a private branch exchange (PBX) or VoIP phone system.
- Work with local phone service companies to make sure no single analog phone lines are installed.
- Block unidentified calls (i.e., calls that appear on caller ID screens as "unknown") from entering your phone system.
- Watch call-detail record (CDR) reports from PBX and VoIP phone systems for rogue phone numbers and abnormal call patterns.

- **VPN routers, VPN firewalls, or VPN concentrators**—Remote access VPN tunnels end at the VPN router, VPN firewall or VPN concentrator, usually within the LAN-to-WAN Domain. All data are encrypted between the VPN client (remote laptop) and the VPN router, firewall, or concentrator—hence the name *tunnel*.
- **Secure Sockets Layer (SSL)/VPN web server**—SSL uses 128-bit encryption between a safe HTTPS webpage and a safe browser. This encrypted VPN tunnel gives end-to-end privacy for remote webpage data sharing.
- **Authentication server**—A server that performs a second-level authentication to verify users seeking remote access.
- **Responsibilities**—The network engineer or WAN group is usually in charge of the Remote Access Domain. This includes both the hardware components and logical elements. Network engineers and security practitioners are in charge of applying security controls according to policies. These include maintaining, updating, and troubleshooting the hardware and logical remote access connection for the Remote Access Domain. This requires management of the following:
  - IP routers
  - IP stateful firewalls
  - VPN tunnels
  - Security monitoring devices
  - Authentication servers
- **Accountability**—Your organization's WAN network manager is accountable for the Remote Access Domain. Typically, the director of IT security must ensure that the Remote Access Domain security plans, standards, methods, and guidelines are used.

Risks, Threats, and Vulnerabilities Commonly Found in the Remote Access Domain

Remote access is dangerous yet necessary for mobile workers. This is true for organizations that rely on a mobile workforce such as sales reps, consultants, and support staff. As organizations cut costs, many urge staff to work from home. The WAN in this case is the public Internet. Making those connections secure is a top job. You will use your organization's strict data classification standard to verify users and encrypt data.

Remote access security controls must use the following:

- **Identification**—The process of providing identifying information, such as a username, a logon ID, or an account number.
- **Authentication**—This is the process for proving that a remote user is who the user claims to be. The most common authentication method is supplying a password. Many organizations use second-level verifying services, such as a **token** (hardware or software), **biometric** fingerprint reader, or smart card. A token can be a hardware device that sends a random number or a software token that text-messages a number to the user. A biometric fingerprint reader grants access only when the user's fingerprint is matched with one stored in the system. A smart card is like a credit card that acts similar to a token. It has a microprocessor chip that verifies the user with a smart-card reader.
- **Authorization**—The process of granting rights to use an organization's IT assets, systems, applications, and data to a specific user.

TABLE 1-8 Risks, threats, vulnerabilities, and mitigation plans for the Remote Access Domain.

RISK, THREAT, OR VULNERABILITY	MITIGATION
Brute-force user ID and password attacks	Establish user ID and password policies requiring periodic changes (i.e., every 30 or 60 days). Passwords must be used, passwords must have more than eight characters, and users must incorporate numbers and letters.
Multiple logon retries and access control attacks	Set automatic blocking for attempted logon retries (e.g., block user access after three logon attempts have failed).
Unauthorized remote access to IT systems, applications, and data	Apply first-level (i.e., user ID and password) and second-level (i.e., tokens, biometrics, and smart cards) security for remote access to sensitive systems, applications, and data.
Private data or confidential data compromised remotely	Encrypt all private data within the database or hard drive. If data are stolen, the thief cannot use or sell it because it will be encrypted.
Data leakage in violation of existing data classification standards	Apply security countermeasures in the LAN-to-WAN Domain, including data leakage security-monitoring tools and tracking, as per your organization's data classification standard.
A mobile worker's laptop is stolen	Encrypt the data on the hard drive if the user has access to private or confidential data. Apply real-time lockout rules when told of a lost or stolen laptop by a user.
Mobile worker token or other authentication stolen	Apply real-time lockout procedures if a token is lost or a device is compromised.

- **Accountability**—The process of recording user actions. The recorded information is often used to link users to system events.

TABLE 1-8 lists Remote Access Domain risks, threats, and vulnerabilities as well as risk-mitigation strategies.

System/Application Domain

The System/Application Domain holds all the mission-critical systems, applications, and data. Authorized users may have access to many components in this domain. Secure access may require second-level checks.

Examples of applications that may require second-level authentication include the following:

- **Human resources and payroll**—Only staff who work on payroll services need access to this private data and confidential information.
- **Accounting and financial**—Executive managers need access to accounting and financial data to make sound business decisions. Securing financial data requires unique security controls with access limited to those who need it. Publicly traded companies are subject to Sarbanes-Oxley (SOX) compliance law requiring security.
- **Customer relationship management (CRM)**—Customer service reps need real-time access to information that includes customer purchasing history and private data.

Technical TIP

Security controls keep private data and intellectual property safe. Encrypting data can stop bogus users. Hackers looking for data know where people hide it and how to find it. Encrypting the data within databases and storage devices gives an added layer of security.

- **Sales order entry**—Sales professionals need access to the sales order-entry and order-tracking system. Private customer data must be kept safe.
- **U.S. military intelligence and tactics**—U.S. military commanders who make decisions on the battlefield use highly sensitive information. Access to that information must meet U.S. Department of Defense (DoD) data classification standards.

The System/Application Domain represents the seventh layer of defense.

System/Application Domain Roles, Responsibilities, and Accountability

Here's an overview of what should go on in the System/Application Domain:

- **Roles and tasks**—The System/Application Domain consists of hardware, operating system software, applications, and data. This domain includes hardware and its logical design. An organization's mission-critical applications and intellectual property assets are here. It must be secured both physically and logically.

  We limited the scope of the System/Application Domain to reducing risks. These include the following:
  - **Physical access to computer rooms, data centers, and wiring closets**—Set up procedure to allow staff to enter secured area.
  - **Server architecture**—Apply a converged server design that employs server blades and racks to combine their use and reduce costs.
  - **Server operating systems and core environments**—Reduce the time that operating system software is open to attack by installing software updates and patches.
  - **Virtualization servers**—Keep physical and logical virtual environments separate and extend layered security solutions into the cloud. Virtualization allows you to load many operating systems and applications using one physical server.
  - **System administration of application servers**—Provide ongoing server and system administration for users.
  - **Data classification standard**—Review data classification standards, procedures, and guidelines on proper handling of data. Maintain safety of private data while in transport and in storage.
  - **Software development life cycle (SDLC)**—Apply secure software development life cycle tactics when designing and developing software.
  - **Testing and quality assurance**—Apply sound software testing, penetration testing, and quality assurance to fill security gaps and software weaknesses.
  - **Storage, backup, and recovery procedures**—Follow data storage, backup, and recovery plans as set by the data classification standard.

    - **Data archiving and retention**—Align policies, standards, procedures, and guidelines to digital storage and retention needs.
    - **Business continuity plan (BCP)**—Conduct a business impact analysis (BIA) and decide which computer uses are most important. Define RTOs for each system. Prepare a BCP focused on those things that are most important for the business to keep going.
    - **Disaster recovery plan (DRP)**—Prepare a disaster recovery plan based on the BCP. Start DRP elements for the most important computer systems first. Organize a DRP team and a remote data center.
- **Responsibilities**—The responsibility for System/Application Domain lies with the director of systems and applications and the director of software development. This domain includes the following:
    - Server systems administration
    - Database design and management
    - Designing access rights to systems and applications
    - Software development
    - Software development project management
    - Software coding
    - Software testing
    - Quality assurance
    - Production support
- **Accountability**—The directors of systems and applications and software development are accountable for the organization's production systems and uses. Typically, the director of IT security is accountable for ensuring that the System/Application Domain security policies, standards, procedures, and guidelines are in compliance.

Risks, Threats, and Vulnerabilities Commonly Found in the System/Application Domain

The System/Application Domain is where the organization's data are like treasure. They can be private customer data, intellectual property, or national security information. They are what attackers seek deep within an IT system. Protecting this treasure is the goal of every organization. Loss of data is the greatest threat in the System/Application Domain.

With a data classification standard, types of data can be isolated in like groups. The more important the data, the deeper you should hide and store them. Consider encrypting data to be stored for a long time. **TABLE 1-9** lists common System/Application Domain risks, threats, and vulnerabilities as well as risk-mitigation strategies.

Weakest Link in the Security of an IT Infrastructure

The user is the weakest link in security. Even information systems security practitioners can make mistakes. Human error is a major risk and threat to any organization. No group can completely control any person's behavior. For these reasons, every organization must be prepared for malicious users, untrained users, and careless users.

TABLE 1-9 Risks, threats, vulnerabilities, and mitigation plans for the System/Application Domain.

RISK, THREAT, OR VULNERABILITY	MITIGATION
Unauthorized access to data centers, computer rooms, and wiring closets	Apply policies, standards, procedures, and guidelines for staff and visitors to secure facilities.
Downtime of servers to perform maintenance	Create a system that brings together servers, storage, and networking.
Server operating systems software vulnerability	Define vulnerability window for server operating system environments. Maintain hardened production server operating systems.
Insecure cloud computing virtual environments by default	Implement virtual firewalls and server segmentation on separate VLANs. A virtual firewall is a software-based firewall used in virtual environments.
Susceptibility of client/server and web applications	Conduct rigorous software and web application testing and penetration testing prior to launch.
Unauthorized access to systems	Follow data classification standards regarding stringent use of second-level authentication.
Data breach where private data of individuals are compromised	Separate private data elements into different databases. For archiving purposes, encrypt sensitive data at rest within databases and storage devices.
Loss or corruption of data	Implement daily data backups and offsite data storage for monthly data archiving. Define data recovery procedures based on defined recovery time objectives (RTOs).
Loss of backed-up data as backup media are reused	Convert all data into digital data for long-term storage. Retain backups from offsite data vaults based on defined RTOs.
Recovery of critical business functions potentially too time-consuming to be useful	Develop a business continuity plan for mission-critical applications providing tactical steps for maintaining availability of operations.
Downtime of IT systems for an extended period after a disaster	Develop a disaster recovery plan specific to the recovery of mission-critical applications and data to maintain operations.

The following strategies can help reduce risk:

- Check the background of each job candidate carefully.
- Give each staff member a regular evaluation.
- Rotate access to sensitive systems, applications, and data among different staff positions.
- Apply sound application and software testing and review for quality.
- Regularly review security plans throughout the seven domains of a typical IT system.
- Perform annual security control audits.

To build a respected and effective profession, information systems security professionals must operate ethically and comply with a code of conduct. This section explains why this tenet is the basis of the profession.

Request for Comments (RFC) 1087: Ethics and the Internet

IAB Statement of Policy

The Internet is a national facility, of which the utility is largely a consequence of its wide availability and accessibility. Irresponsible use of this critical resource poses an enormous threat to its continued availability to the technical community. The U.S. government sponsors of this system have a fiduciary responsibility to the public to allocate government resources wisely and effectively. Justification for the support of this system suffers when highly disruptive abuses occur. Access to and use of the Internet are privileges and should be treated as such by all users of this system.

The IAB strongly endorses the view of the Division Advisory Panel of the National Science Foundation Division of Network, Communications Research and Infrastructure, which, in paraphrase, characterized as unethical and unacceptable any activity which purposely:

(a) seeks to gain unauthorized access to the resources of the Internet,

(b) disrupts the intended use of the Internet,

(c) wastes resources (people, capacity, computer) through such actions,

(d) destroys the integrity of computer-based information, and/or

(e) compromises the privacy of users.

Ethics and the Internet

Imagine if there were no air traffic controllers and airplanes flew freely. Trying to take off and land would be extremely dangerous. There would probably be many more accidents. Such a situation would wreak havoc.

Incredibly, cyberspace has no authorities that function like air traffic controllers. To make matters worse, human behavior online often is less mature than in normal social settings. Cyberspace has become the new playground for today's bad guys. This is why the demand for systems security professionals is growing so rapidly.

The U.S. government and the Internet Architecture Board (IAB) has defined a policy regarding acceptable use of the Internet geared toward U.S. citizens. It is not a law or a mandate, however; because cyberspace is global and entirely without borders, this policy cannot be enforced. Its use is based on common sense and personal integrity. The sidebar presents the IAB's standard of ethics and the Internet.

Ethics are a matter of personal integrity. The systems security profession is about doing what is right and stopping what is wrong. Use of the Internet is a privilege shared by all. It is a communications medium with no borders, no cultural bias, and no prejudice. Users have the privilege to connect. This is something to be thankful for. Unfortunately, bad guys use cyberspace to commit crimes and cause trouble. This has created a global need for systems security professionals.

IT Security Policy Framework

Cyberspace cannot continue to flourish without some assurances of user security. Several laws now require organizations to keep personal data private. Businesses cannot operate

effectively on an Internet where anyone can steal their data. IT security is crucial to any organization's ability to survive. This section introduces you to an IT security policy framework. The framework consists of policies, standards, procedures, and guidelines that reduce risks and threats.

Definitions

An IT security policy framework contains four main components:

- **Policy**—A policy is a short written statement that the people in charge of an organization have set as a course of action or direction. A policy comes from upper management and applies to the entire organization.
- **Standard**—A standard is a detailed written definition for hardware and software and how they are to be used. Standards ensure that consistent security controls are used throughout the IT system.
- **Procedures**—These are written instructions for how to use policies and standards. They may include a plan of action, installation, testing, and auditing of security controls.
- **Guidelines**—A guideline is a suggested course of action for using the policy, standards, or procedures. Guidelines can be specific or flexible regarding use.

FIGURE 1-10 is an example of a hierarchical IT security policy framework. Policies apply to an entire organization. Standards are specific to a given policy. Procedures and guidelines help define use. Within each policy and standard, identify the impact for the seven domains of a typical IT infrastructure. This will help define the roles, responsibilities, and accountability throughout.

Foundational IT Security Policies

The focus of your organization's IT security policy framework is to reduce your exposure to risks, threats, and vulnerabilities. It is important to relate policy definition and standards to practical design requirements. These requirements will properly apply the best security controls and countermeasures. Policy statements must set limits as well as refer to standards, procedures, and guidelines. Policies define how security controls and countermeasures must be used to comply with laws and regulations.

Examples of some basic IT security policies include the following:

- **Acceptable use policy (AUP)**—The AUP defines the actions that are and are not allowed with respect to the use of organization-owned IT assets. This policy is specific to the User Domain and mitigates risk between an organization and its employees.

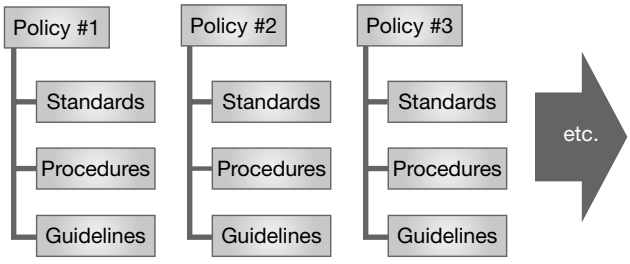


FIGURE 1-10
Hierarchical IT security policy framework.

- **Security awareness policy**—This policy defines how to ensure that all personnel are aware of the importance of security and behavioral expectations under the organization's security policy. This policy is specific to the User Domain and is relevant when you need to change organizational security awareness behavior.
- **Asset classification policy**—This policy defines an organization's data classification standard. It tells what IT assets are critical to the organization's mission. It usually defines the organization's systems, uses, and data priorities and identifies assets within the seven domains of a typical IT infrastructure.
- **Asset protection policy**—This policy helps organizations define a priority for mission-critical IT systems and data. This policy is aligned with an organization's **business impact analysis (BIA)** and is used to address risks that could threaten the organization's ability to continue operations after a disaster.
- **Asset management policy**—This policy includes the security operations and management of all IT assets within the seven domains of a typical IT infrastructure.
- **Vulnerability assessment and management**—This policy defines an organization-wide vulnerability window for production operating system and application software. You develop organization-wide vulnerability assessment and management standards, procedures, and guidelines from this policy.
- **Threat assessment and monitoring**—This policy defines an organization-wide threat assessment and monitoring authority. You should also include specific details regarding the LAN-to-WAN Domain and AUP compliance in this policy.

Organizations need to tailor their IT security policy framework to their environment. After conducting a security assessment of their IT setup, many organizations align policy definitions to gaps and exposures. Policies typically require executive management and general legal counsel review and approval.

Data Classification Standards

The goal and objective of a data classification standard is to provide a consistent definition for how an organization should handle and secure different types of data. Security controls protect different data types. These security controls are within the seven domains of a typical IT infrastructure. Procedures and guidelines must define how to handle data within the seven domains of a typical IT infrastructure to ensure data security.

For businesses and organizations under recent compliance laws, data classification standards typically include the following major categories:

- **Private data**—Data about people that must be kept private. Organizations must use proper security controls to be in compliance.
- **Confidential**—Information or data owned by the organization. Intellectual property, customer lists, pricing information, and patents are examples of confidential data.
- **Internal use only**—Information or data shared internally by an organization. Although confidential information or data may not be included, communications are not intended to leave the organization.
- **Public domain data**—Information or data shared with the public such as website content, white papers, and the like.

U.S. Federal Government Data Classification Standard

The U.S. government, under Executive Order 13526, defines a data classification standard for all federal government agencies, including the Department of Defense (DoD). President Barack Obama signed this executive order on December 9, 2009. Although the U.S. government and its citizens enjoy the free flow of information, securing information is essential for national security, defense, or military action.

The following points define the U.S. federal government data classification standards:

- **Top secret**—Applies to information that the classifying authority finds would cause grave damage to national security if it were disclosed.
- **Secret**—Applies to information that the classifying authority finds would cause serious damage to national security if it were disclosed.
- **Confidential**—Applies to information that the classifying authority finds would cause damage to national security.

Whereas public-domain information is considered unclassified, it is not part of the data classification standard.

The U.S. government does have rules for handling unclassified (posing no threat to national security if exposed) and controlled unclassified information (for official use only, sensitive but unclassified, and law enforcement sensitive). Note that these rules are not included in Executive Order 13562 and were based on previous standards put into use by the administration of President George W. Bush.

Depending on your organization's data classification standard, you may need to encrypt data of the highest sensitivity even in storage devices and hard drives. For example, you may need to use encryption and VPN technology when using the public Internet for remote access. But internal LAN communications and access to systems, applications, or data may not require use of encryption.

Users may also be restricted from getting to private data of customers and may be able to access only certain pieces of data. Customer service reps provide customer service without getting to all of a customer's private data. For example, they may not be able to see the customer's entire Social Security number or account numbers; only the last four digits may be visible. This method of hiding some of the characters of the sensitive data element is called **masking**.

Technical TIP

Organizations should start defining their IT security policy framework by defining an asset classification policy. This policy, in turn, aligns itself directly to a data classification standard. This standard defines the way an organization is to secure and protect its data. Working from your data classification standard, you need to assess whether any private or confidential data travels within any of the seven domains of a typical IT infrastructure. Depending on how you classify and use the data, you will need to employ appropriate security controls throughout the IT infrastructure.

CHAPTER SUMMARY

This chapter introduced information systems security and the systems security profession. You saw a common definition for a typical IT infrastructure. You learned about risks, threats, and vulnerabilities within the seven domains. Each of these domains requires the use of strategies to reduce risks, threats, and vulnerabilities. You saw how IT security policy frameworks can help organizations reduce risk by defining authoritative policies. You also learned that data classification standards provide organizations with a road map for ways to handle different types of data. But who is going to implement the security controls?

Qualified IT security professionals are required to design and implement the appropriate security controls and countermeasures. As an IT security professional, you must have the highest human integrity and ethics. There are several professional security certifications available to security professionals. CompTIA's Security+ professional certification is foundational to entry level IT security professionals. $(ISC)^2$, the **International Information Systems Security Certification Consortium**, offers the **Certified Information Systems Security Professional CISSP®** certification for more experienced professionals. Obtaining the CISSP® professional certification requires the following: passing a certification exam, having at least five years of experience working in the information system security field, adhering to a code of ethics, and submitting continuing professional education (CPE) credits to maintain your certification.

KEY CONCEPTS AND TERMS

Acceptable use policy (AUP)
Application gateway firewalls
Availability
Biometric
BlackBerry
Business continuity plan (BCP)
Business impact analysis (BIA)
Carrier Sense Multiple Access/Collision Detection (CSMA/CD)
Certified Information Systems Security Professional (CISSP)
Children's Internet Protection Act (CIPA)
Ciphertext
Cleartext
Confidentiality
Content filtering
Cryptography
Cybersecurity
Cyberspace
Data breach
Data classification standard
Defense in depth
Demilitarized zone (DMZ)
Disaster recovery plan (DRP)
Downtime
E-commerce
Encryption
End-User License Agreement (EULA)
Ethernet
Family Educational Rights and Privacy Act (FERPA)
Federal Information Security Management Act 2002 (FISMA)
Federal Information Security Modernization Act 2014 (FISMA)
FICO
File Transfer Protocol (FTP)
Generation Y
Gramm-Leach-Bliley Act (GLBA)
Hardening
Health Insurance Portability and Accountability Act (HIPAA)
Hypertext Transfer Protocol (HTTP)
Hypertext Transfer Protocol Secure (HTTPS)
Identity theft
IEEE 802.3 CSMA/CD
Information security
Information systems
Information systems security

KEY CONCEPTS AND TERMS, *continued*

Instant messaging (IM) chat
Institute of Electrical and Electronics Engineers (IEEE)
Integrity
International Information Systems Security Certification Consortium $(ISC)^2$
Internet
Internet of Things (IoT)
Intrusion detection system/intrusion prevention system (IDS/IPS)
IP default gateway router
IP stateful firewall
IT security policy framework
Layer 2 switch
Layer 3 switch
Local area network (LAN)
Malicious code
Malware
Masking
Mean time between failures (MTBF)
Mean time to failure (MTTF)
Mean time to repair (MTTR)
Multiprotocol Label Switching (MPLS)
Network interface card (NIC)
Network keys
Network operations center (NOC)
Personal digital assistant (PDA)
Ping
Protocol
Proxy firewalls
Proxy server
Recovery time objective (RTO)
"RFC 1087: Ethics and the Internet"
Risk
Sarbanes-Oxley Act (SOX)
Secure Sockets Layer virtual private network (SSL-VPN)
Security control
Service level agreement (SLA)
Simple Network Management Protocol (SNMP)
Smartphone
Software vulnerability
Subnet mask address
Telnet
Thick client
Thin client
Threat
Token
Transmission Control Protocol/Internet Protocol (TCP/IP)
Trivial File Transfer Protocol (TFTP)
Trojan
Two-step authentication
Unified communications
Uptime
Virtual LAN (VLAN)
Virtual private network (VPN)
Virus
Vulnerability
Vulnerability assessment
Vulnerability window
Wireless access point (WAP)
Wireless Fidelity (Wi-Fi)
Wireless LAN (WLAN)
Workstation
World Wide Web (WWW)
Worm

CHAPTER 1 ASSESSMENT

1. Information security is specific to securing information, whereas information systems security is focused on the security of the systems that house the information.

A. True
B. False

2. Software manufacturers limit their liability when selling software using which of the following?

A. End-User License Agreements
B. Confidentiality agreements
C. Software development agreements
D. By developing error-free software and code so there is no liability
E. None of the above

3. The _____ tenet of information systems security is concerned with the recovery time objective.

A. Confidentiality
B. Integrity
C. Availability
D. All of the above
E. None of the above

4. If you are a publicly traded company or U.S. federal government agency, you must go public and announce that you have had a data breach and must inform the impacted individuals of that data breach.

A. True
B. False

5. Organizations that require customer service representatives to access private customer data can best protect customer privacy and make it easy to access other customer data by using which of the following security controls?
   A. Preventing customer service representatives from accessing private customer data
   B. Blocking out customer private data details and allowing access only to the last four digits of Social Security numbers or account numbers
   C. Encrypting all customer data
   D. Implementing second-tier authentication when accessing customer databases
   E. All of the above

6. The _____ is the weakest link in an IT infrastructure.
   A. System/Application Domain
   B. LAN-to-WAN Domain
   C. WAN Domain
   D. Remote Access Domain
   E. User Domain

7. Which of the following security controls can help mitigate malicious email attachments?
   A. Email filtering and quarantining
   B. Email attachment antivirus scanning
   C. Verifying with users that email source is reputable
   D. Holding all inbound emails with unknown attachments
   E. All of the above

8. You can help ensure confidentiality by implementing _____.
   A. An acceptable use policy
   B. A data classification standard
   C. An IT security policy framework
   D. A virtual private network for remote access
   E. Secure access controls

9. Encrypting email communications is needed if you are sending confidential information within an email message through the public Internet.
   A. True
   B. False

10. Using security policies, standards, procedures, and guidelines helps organizations decrease risks and threats.
    A. True
    B. False

11. A data classification standard is usually part of which policy definition?
    A. Asset protection policy
    B. Acceptable use policy
    C. Vulnerability assessment and management policy
    D. Security awareness policy
    E. Threat assessment and monitoring policy

12. A data breach is typically performed after which of the following?
    A. Unauthorized access to systems and application is obtained
    B. Vulnerability assessment scan
    C. Configuration change request
    D. Implementation of a new data center
    E. Implementation of a web application update

13. Maximizing availability primarily involves minimizing _____.
    A. The amount of downtime recovering from a disaster
    B. The mean time to repair a system or application
    C. Downtime by implementing a business continuity plan
    D. The recovery time objective
    E. All of the above

14. Which of the following is not a U.S. compliance law or act?
    A. CIPA
    B. FERPA
    C. FISMA
    D. PCI DSS
    E. HIPAA

15. Internet IP packets are to cleartext what encrypted IP packets are to _____.
    A. Confidentiality
    B. Ciphertext
    C. Virtual private networks
    D. Cryptography algorithms
    E. None of the above