INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES

ISSA

Fundamentals of Information Systems Security

FOURTH EDITION

David Kim | Michael G. Solomon

INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES

ISSA

Fundamentals of Information Systems Security

FOURTH EDITION

David Kim | Michael G. Solomon

JONES & BARTLETT
LEARNING

World Headquarters
Jones & Bartlett Learning
25 Mall Road
Burlington, MA 01803
978-443-5000
info@jblearning.com
www.jblearning.com

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

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

24458-8

Production Credits

Vice President, Product Management: Marisa R. Urbano
Vice President, Product Operations: Christine Emerton
Director, Content Management: Donna Gridley
Director, Project Management and Content Services: Karen Scott
Product Manager: Ned Hinman
Content Strategist: Melissa Duffy
Content Coordinator: Mark Restuccia
Development Editor: Kim Lindros
Technical Editor: Jeffrey Parker
Project Manager: Jessica deMartin
Senior Project Specialist: Jennifer Risden
Digital Project Specialist: Rachel DiMaggio
Marketing Manager: Suzy Balk
Product Fulfillment Manager: Wendy Kilborn
Composition: Straive
Cover Design: Briana Yates
Media Development Editor: Faith Brosnan
Rights Specialist: Benjamin Roy
Cover Image (Title Page, Front Matter Opener, Part Opener, Chapter Opener): © Ornithopter/Shutterstock
Printing and Binding: McNaughton & Gunn

Library of Congress Cataloging-in-Publication Data

Names: Kim, David (Information technology security consultant) | Solomon, Michael (Michael G.), 1963– author.
Title: Fundamentals of information systems security / David Kim, Michael G. Solomon.
Description: Fourth edition. | Burlington, Massachusetts : Jones & Bartlett Learning, [2023] | Includes bibliographical references and index.
Identifiers: LCCN 2021021301 | ISBN 9781284220735 (paperback)
Subjects: LCSH: Computer security. | Computer networks—Security measures. | Information storage and retrieval systems—Security measures.
Classification: LCC QA76.9.A25 K536 2023 | DDC 005.8—dc23
LC record available at https://lccn.loc.gov

6048

Printed in the United States of America

25 24 23 22 21 10 9 8 7 6 5 4 3 2 1

This book is dedicated to our readers and students and the IT professionals pursuing a career in information systems security. May your passion for learning IT security help you protect the information assets of the United States of America, our businesses, and the private data of our citizens.
—David Kim

To God, who has richly blessed me in so many ways.
—Michael G. Solomon

Contents

Preface

Purpose of This Text

This text is part of the Information Systems Security & Assurance (ISSA) Series from Jones & Bartlett Learning (*www.issaseries.com*). Designed for courses and curriculums in IT Security, Cybersecurity, Information Assurance, and Information Systems Security, this series features a comprehensive, consistent treatment of the most current thinking and trends in this critical subject area. These titles deliver fundamental information security principles packed with real-world applications and examples. Authored by Certified Information Systems Security Professionals (CISSPs) and experienced cybersecurity consultants, this series delivers comprehensive information on all aspects of information security. Reviewed word for word by leading technical experts in the field, these texts are not just current but forward thinking—putting you in the position to solve the cybersecurity challenges not just of today but also of tomorrow.

Part I of this text on information security fundamentals focuses on new risks, threats, and vulnerabilities associated with the transformation to a digital world and the Internet of Things (IoT). Individuals, students, educators, businesses, organizations, and governments have changed how they communicate, share personal information and media, and do business. Led by the vision of the IoT, the Internet and broadband communications have entered into our everyday lives. This digital revolution has created a need for information systems security. With recent compliance laws requiring organizations to protect and secure private data and reduce liability, information systems security has never been more recognized than it is now.

Part II is adapted from CompTIA's Security+ professional certification. CompTIA's Security+ is the most widely accepted foundational, vendor-neutral IT security knowledge and skills professional certification. As a benchmark for foundational knowledge and best practices in IT security, the Security+ professional certification includes the essential principles for network security, operational security, and compliance. Also covering application, data, and host security, threats and vulnerabilities, access control, identity management, and cryptography, the Security+ certification provides a solid foundation for an IT security career.

Part III of this text provides a resource for readers and students desiring more information on information security standards, education, professional certifications, and recent compliance laws. These resources are ideal for students and individuals desiring additional information about educational and career opportunities in information systems security.

New to This Edition

This new edition has been updated to reflect the security environments you will encounter in today's organizations. The content has been slightly reorganized, extended, and refreshed to ensure that it covers the latest trends, standards, and industry best practices. Part I, The Need for Information Security, covers how today's complex business environments have changed due to technological and cultural influences and how those changes impact security. Part II, Securing Today's Information Systems, continues the discussion from Part I to form the core material of the text. In Part II we dig into the various aspects and domains of cybersecurity and discuss how security applies in each case. This edition retains the technical information from previous editions but frames discussions in the context of satisfying business goals at the strategic level. Additional focus is placed on continuity and emerging strategic concerns. And, finally, Part III, Information Security Standards, Certifications, and Laws, presents an up-to-date overview of various external governance influences that inform security-related decisions and strategy. This latest edition provides the most comprehensive coverage to date of how to implement enterprise security as a strategic organizational objective.

Cloud Labs

This text is accompanied by Cybersecurity Cloud Labs. These hands-on virtual labs provide immersive mock IT infrastructures where students can learn and practice foundational cybersecurity skills as an extension of the lessons in this text. For more information or to purchase the labs, visit *go.jblearning.com/Kim4e*.

Learning Features

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

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

Audience

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

Acknowledgments

I would like to thank Michael Solomon, for taking the lead authoring role on this fourth edition, and to the Jones & Bartlett Learning team led by Ned Hinman. This journey that we have been on together from the first to the fourth edition has allowed us to significantly impact the lives of new cybersecurity professionals across the country as well as protect our information assets.

This fourth edition book project commenced during the COVID-19 pandemic, which prevented me from being able to physically visit and spend quality time with my mom, Mrs. Yum Kim.

I would like to thank my mom for her unconditional love and for guiding me into the man I have become.

David Kim

I would like to thank David Kim and the whole Jones & Bartlett Learning team for providing pertinent editorial comments and for helping to fine-tune the book's content. All of you made the process so much easier and added a tremendous amount of value to the book. I want to thank God for blessing me so richly with such a wonderful family, and for my family's support throughout the years. My best friend and wife of over three decades, Stacey, is my biggest cheerleader and supporter through many professional and academic endeavors. I would not be who I am without her.

Both of our sons have always been sources of support and inspiration. To Noah, who still challenges me, keeps me sharp, and tries to keep me relevant, and Isaac, who left us far too early. We miss you, son.

Michael G. Solomon

The Authors

David Kim is the president of Security Evolutions, Inc. (SEI; *www.security-evolutions.com*) located outside the Washington, DC, metropolitan area. SEI provides governance, risk, and compliance consulting services for public and private sector clients globally. SEI's clients include health care institutions, banking institutions, governments, and international airports. SEI's IT security consulting services include security risk assessments, vulnerability assessments, compliance audits, and designing of layered security solutions for enterprises. In addition, available services include developing business continuity and disaster recovery plans. Mr. Kim's IT and IT security experience encompasses more than 30+ years of technical engineering, technical management, and sales and marketing management. This experience includes LAN/WAN; internetworking; enterprise network management; and IT security for voice, video, and data networking infrastructures. He is an accomplished author and part-time adjunct professor who enjoys teaching cybersecurity to students across the United States.

Michael G. Solomon, PhD, CISSP, PMP, CISM, CySA+, Pentest+, is an author, educator, and consultant focusing on privacy, security, blockchain, and identity management. As an IT professional and consultant since 1987, Dr. Solomon has led project teams for many Fortune 500 companies and has authored and contributed to more than 25 books and numerous training courses. Dr. Solomon is a professor of cyber security at the University of the Cumberlands and holds a PhD in computer science and informatics from Emory University.

PART I

The Need for Information Security

CHAPTER

1

Information Systems Security

THE WORLDWIDE NETWORK WE KNOW AS THE INTERNET HAS DEMONSTRATED phenomenal growth and change from its humble beginnings. Once merely a tool used by a small number of universities and government agencies, it is truly a global network with 5 billion users. As it has grown, it has changed the way people, and even devices, communicate and do business, creating untold opportunities and benefits. Today, the Internet continues to grow and expand in new and varied ways. It supports innovation and new services, such as real-time streaming and cloud computing. When the Internet started, the majority of connected devices were computers, whether for personal use or within a company. In the most recent years, however, an increasing variety of devices beyond computers, including smartphones, tablets, vehicles, appliances, doorbells, vending machines, drones, smart homes, and smart buildings, can connect and share data.

The Internet as we know it today is experiencing a growth spurt as the Internet of Things (IoT) spreads and impacts our daily lives. Although the Internet officially started in 1969, the extent to which people have come to depend on it is new. Today, people interact with the Internet and cyberspace as part of normal day-to-day living. In fact, not being connected to the Internet is often seen as annoying for both personal and business use. Users now face privacy and security issues regarding their personal and business information as intelligent and aggressive cybercriminals, terrorists, and scam artists increasingly and continuously lurk in the virtual shadows. Connecting computers and devices to the Internet immediately exposes them to attack, from which frustration and hardship can result. 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 or disrupt military communication.

You can make a difference. The world needs people who understand cybersecurity and can protect computers, devices, and networks from cybercriminals. Remember, it's all about protecting sensitive data and the infrastructure around 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 information technology (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 approximately 5 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 locate documents and resources on different computers and link them together across a set of connected networks. 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 a network of computers. The name of this system is the **World Wide Web (WWW)** , which is also known as **cyberspace** or simply 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; and cyberspace is all the accessible users, networks, webpages, and applications working in this worldwide electronic realm.

Recent Data Breaches in the United States (2014–2020)

Each year the number of reported **data breaches** around the world grows, along with the damage they cause individuals and organizations. Both the public and the private sectors 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.

ORGANIZATION	DATA BREACH	IMPACT OF DATA BREACH
Yahoo	Yahoo disclosed in December 2016 that a group of hackers compromised 1 billion accounts. In October 2017, Yahoo released more information and increased the estimate of breached accounts to 3 billion.	As a result of the Yahoo breach, all Yahoo users were urged to change their passwords and update related security questions. Users were also discouraged from reusing passwords and to immediately change any passwords of other accounts that shared the disclosed Yahoo passwords.
First American Financial Corporation	About 885 million users had sensitive personal financial data leaked in May 2019. Hackers were able to extract data that included transactions dating back to 2003.	Customers were immediately at a higher risk of identity theft because their personal financial data had been breached, and that risk continues.
Verifications.io	In February 2019, 763 million unique user email addresses of the Verifications.io validation service were leaked along with names, telephone numbers, Internet Protocol (IP) addresses, birthdates, and gender.	As with the First American breach, Verifications.io customers were (and still are) exposed to an elevated risk of becoming a victim of identity theft.
Marriott/ Starwood Hotels	The Starwood Hotels and Resorts information system was compromised in 2014, but the breach wasn't detected until 2018. The hackers silently collected customer data for four years. In the end, Starwood estimated that 500 million guests had personal information stolen, including passport information and payment card numbers for as many as 100 million customers, although payment card information was encrypted.	Two years before the Starwood breach was discovered, Marriott International acquired Starwood. Marriott had to deal with the large-scale loss of customer confidence and was forced to invest an undisclosed amount to reassure its customers of its privacy and security policies.

ORGANIZATION	DATA BREACH	IMPACT OF DATA BREACH
	In May 2018, the Twitter social media platform announced that a software bug had resulted in user passwords being stored in an unencrypted log file location, making them accessible to hackers. Twitter strongly recommended that all 300 million users change their passwords but never disclosed how many accounts were actually affected by the breach.	Because many social media users use the same passwords on multiple sites, a password disclosure on one site could allow hackers to compromise accounts on multiple sites. Even with good password practices, a social media breach can disclose personal information that can be used for additional attacks, including identity theft.
FireEye	In December 2020, security firm FireEye announced its penetration testing tools, used to assess clients' data security, were stolen.	Given the purpose of FireEye's proprietary tools, FireEye warned that its tools could be used to maliciously hack into other companies.

Unfortunately, when you connect to cyberspace, you also open the door to a lot of bad actors who want to find and steal your data. Every computer or device that connects to the Internet is at risk, creating an IoT, which supports users in all aspects of their lives. Like outer space, the maturing Internet is a new frontier, and it has no Internet government or central authority. It is full of opportunities and challenges—and questionable behavior. Across the globe, 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 working on behalf of other nations. The quantity of cyberattacks on national interests is increasing.

With the IoT now connecting personal and home devices, as well as vehicles, to the Internet, even more data is available to steal, making it imperative for all users to 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., Social Security and credit card numbers), and protection of our own data is the responsibility of all of us. **FIGURE 1-1** illustrates this new frontier.

The components that make up cyberspace are not automatically secure. Such components include cabling, physical networking devices, 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 most common version of the communications **protocol** (i.e., a list of rules and methods for communicating across the Internet)—the **Transmission Control Protocol/Internet**

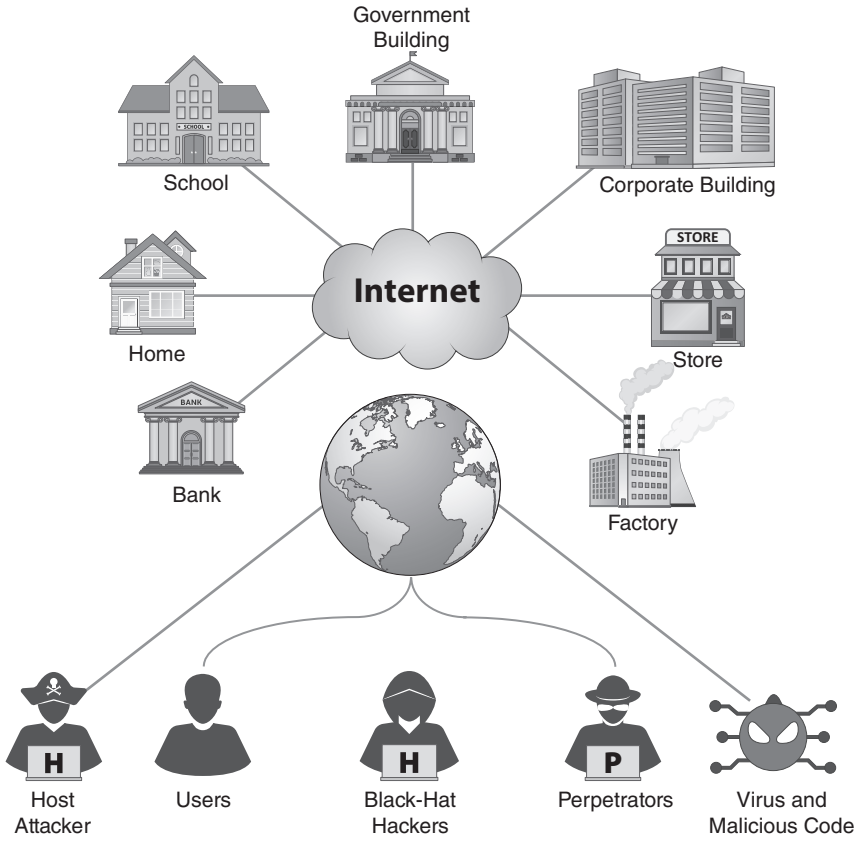


FIGURE 1-1
Cyberspace: The new frontier.

Protocol (TCP/IP). TCP/IP is not just one protocol but rather a suite of protocols developed for communicating across a network. Named after the two most important protocols, TCP/IP protocols work together to allow any two computers to be connected, in order to communicate, and thus create a network. TCP/IP breaks messages into chunks, or packets, to send data between networked computers. The data security problem lies in the fact that the data is readable within each IP packet, using simple software available to anyone. This readable mode is known as **cleartext**. That means the data sent inside a TCP/IP packet must be hidden or encrypted 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 does everyone connect to it so willingly and add to its growth? The answer is the huge growth of the web from the mid-1990s to the early 2000s and the relatively low perceived risk of getting online. Connecting to the Internet gave anyone instant access to the web and its many resources. In the early years of the web, cybercrime was rare, and most users felt safe and anonymous online. The appeal of easy, worldwide connectivity drove the demand to connect. This demand and subsequent growth helped drive costs lower for high-speed

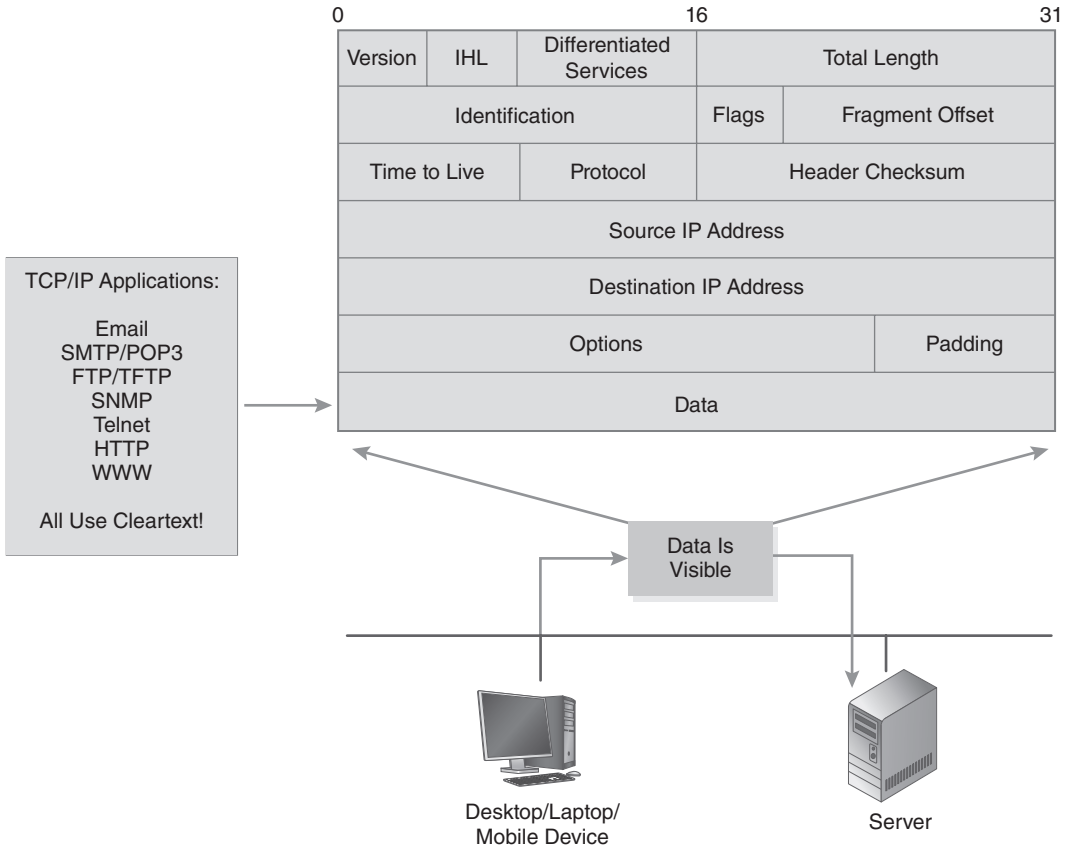


FIGURE 1-2
TCP/IP communications are in cleartext.

communications. Households, businesses, and governments gained affordable high-speed Internet access, and, as wireless and cellular connections have become more common and affordable, staying connected has become easier no matter where you are and what devices you need to connect. **FIGURE 1-3** shows how the IoT is making the world digitally connected. The IoT magnifies the risk, threat, and vulnerability issues, given that a hacker or an attacker can gain unauthorized access to any IP-connected device. Once access to an IP-connected device has been granted, data can be stolen or damage done if the attacker so desires. This "dark villain" nature of a hacker is what helped label hackers as "black hats."

Internet growth has also been driven by generational differences. The Generation Y (people born between 1981 and 1996, also called Millennials) culture came into prominence as baby boomers began to retire. This new generation of people grew up with cell phones, **smartphones**, and increasingly available Internet access. There is even a newer named generation, Generation Z (people born between 1997 and 2012), who have

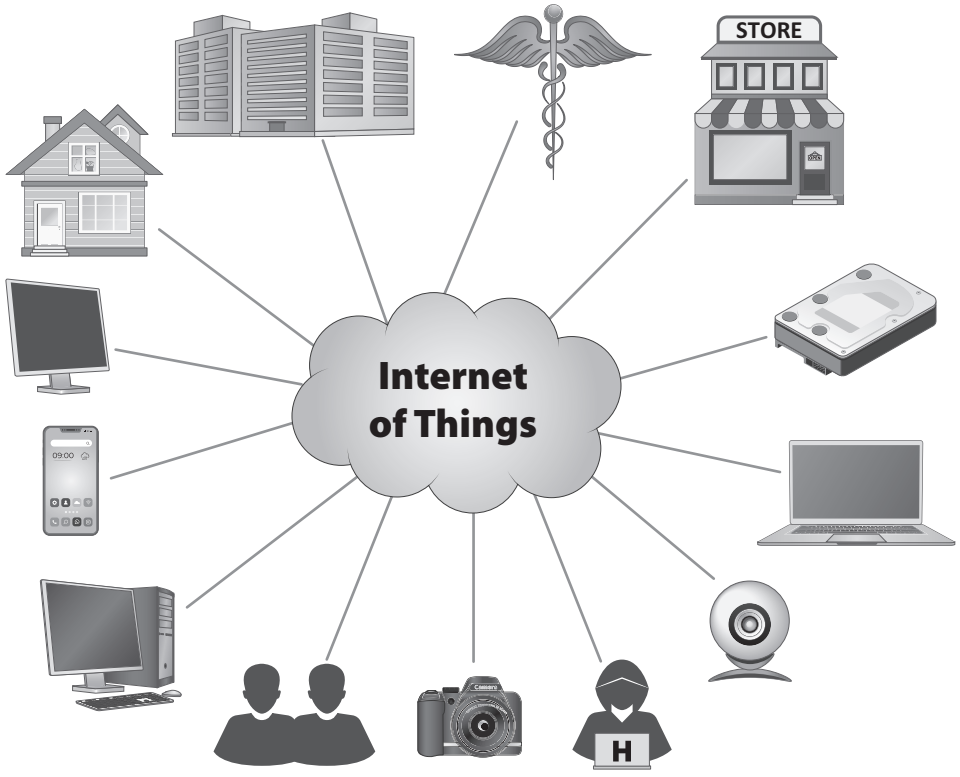


FIGURE 1-3
Internet of Things (IoT) supports any-to-any connectivity.

never known a life without smartphones and nearly constant connectivity and real-time communication. Today's personal communications include Voice over Internet Protocol (VoIP), text messaging, and social media as well as audio conferencing 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™, Zoom™, Adobe Connect™, 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—in the local area and around the world—and seeks sensitive data. Thus, the name of the game for an attacker is to gain unauthorized access, which means that the attacker obtains users' authorized logon IDs and passwords without their permission. Using those logon credentials, the attacker gains access to all the systems and applications that the users' access permits. If unauthorized access is granted, then sensitive data may be accessible and can be downloaded, depending on that user's access controls. For this reason, IT infrastructures need proper security controls. Because of the information security war, a great demand has been created for information systems

security and information assurance professionals, who represent a new kind of cyber-warrior to help defend security and business interests.

Risks, Threats, and Vulnerabilities

This text 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 as secure as possible, first, you first need to understand the concepts of risks, threats, and vulnerabilities.

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

- Losing access to data
- Losing business because a disaster has destroyed the building in which the business operates
- Failing to comply with laws and regulations

A **threat** is any action, either natural or human induced, that could damage an asset. Natural threats include floods, earthquakes, and severe storms, all of which require organizations to create plans to ensure that business operations can continue (i.e., a business continuity plan [BCP]) and the organization can recover (i.e., disaster recovery plan [DRP]). A BCP prioritizes the functions an organization needs to keep going, and a 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, and malicious code, or malware, is a computer program written to cause a specific action to occur, such as erasing a hard drive. Threats can harm an individual, a business, or an 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. On the one hand, if you were cooking a meal on a grill, you would need to light a fire in the grill, which is designed to contain the fire so that the fire poses no danger if the grill is used properly. On the other hand, lighting a fire in a computer data center will likely cause damage because a computer data center is vulnerable to fire, whereas a grill is not. Therefore, 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. Because computers must run software to be useful and 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 installs the software. All software vendors use EULAs, which means that the burden of protecting IT systems and data lies with internal information systems security professionals.

End-User License Agreements (EULAs)

EULAs are license agreements between a user and a software vendor. EULAs are used to protect software vendors from claims arising from the behavior of imperfect software and typically contain a warranty disclaimer, which limits the vendors' 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 $5 (U.S.), 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.

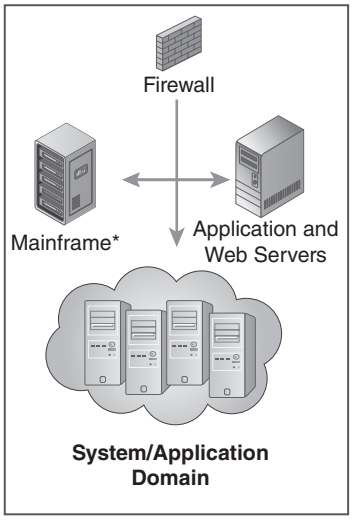
Used with permission from Microsoft.

What Is Information Systems Security?

The easiest way to define information systems security is to break it into its component parts. 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. **Security** is being free from danger or risk. Since there is always some amount of risk present, achieving security is aspirational, not absolute. 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, and organizations must address this need head-on. **FIGURE 1-4** reviews the types of information commonly found within an IT infrastructure.

Compliance Laws and Regulations Drive the Need for Information Systems Security

Cyberspace brings new threats to people and organizations. Individuals need to protect their privacy, and businesses and organizations are responsible for protecting both their



- 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?

intellectual property and any personal or private data they handle. Various laws require organizations to use security controls to protect private and confidential data. Current laws and regulations related to information security include the following:

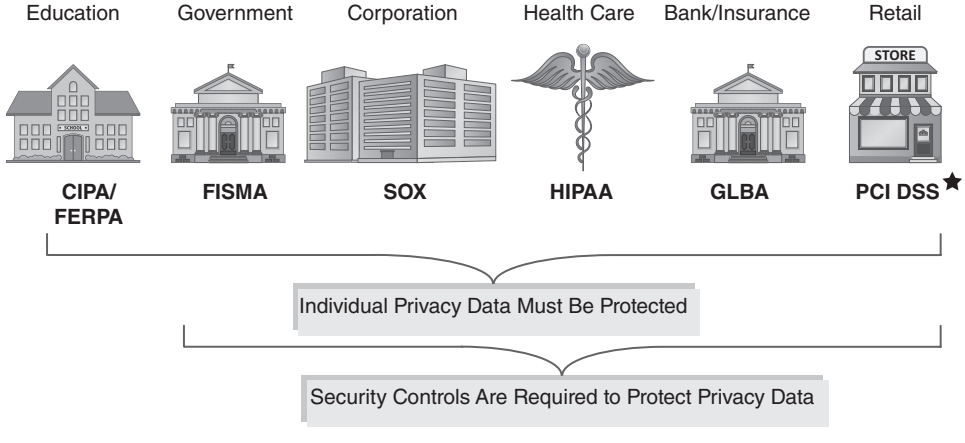
- **Federal Information Security Management Act (FISMA)**—Passed in 2002, FISMA requires federal civilian agencies to provide security controls over resources that support federal operations.
- **Federal Information Security Modernization Act (FISMA)**—Passed in 2014, FISMA was enacted to update FISMA 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 implement security and privacy controls 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 they are using email, chatrooms, and other electronic communications
  - Restricting hacking and other unlawful activities by children online
  - Prohibiting the disclosure and distribution of personal information about children without permission
  - Restricting children's access to harmful materials
  - Warning children on the use and dangers of social media
- **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.

All of the compliance laws listed so far are U.S. laws, but the United States is not the only place legislators are concerned about security and privacy. Many nations are busy crafting laws and regulations to protect organizations and consumers from cybercriminals. One of the most recent and wide-ranging attempts to protect personal data privacy is the European Union's (EU's) **General Data Protection Regulation (GDPR)**. GDPR is a regulation in EU law that protects each EU citizen's individual data. GDPR gives individuals ownership of their personal data and limits how that data can be collected and used. Although GDPR is an EU regulation, it covers data that flows into and out of EU information systems. Any organization in the world that handles EU citizen data is required to comply with GDPR.

FIGURE 1-5
Compliance laws and regulations drive the need for information systems security.



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 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.

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. However, you'll most commonly see C-I-A in information security refer to the security triad, or tenets of security.

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 **confidentiality, integrity, and availability (C-I-A)** triad to define the organization's security baseline goals for a typical IT infrastructure. Once defined, these goals will translate into security controls and requirements based on the type of data being protected.

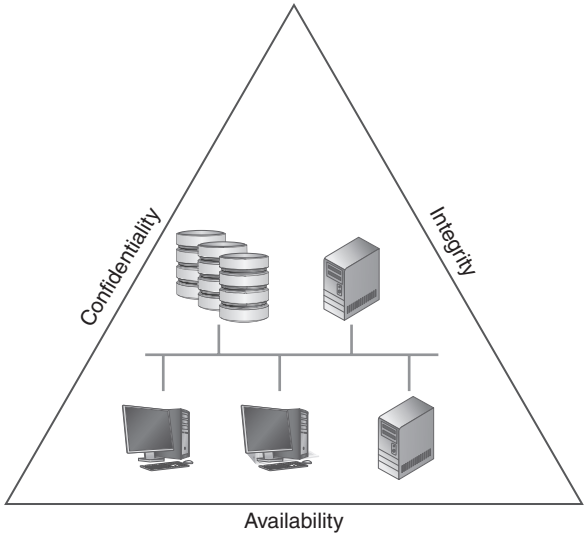


FIGURE 1-6
The three tenets of information systems security.

Identity Theft

Identity theft affects about 15 million U.S. citizens each year, with financial losses costing upward of $50 billion, and is a major threat to U.S. consumers. Many elements make up a person's identity, including but 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, impostors can access people's accounts with just their 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 someone's private data and financial account information to be compromised. To reduce the possibility of loss, these documents should be shredded before they are discarded.

Identity theft extends beyond mere financial loss to damaging your Fair Isaac Corp. (**FICO**) personal credit rating, which 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 that 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 individuals' private data require businesses and organizations to have proper security controls to ensure confidentiality.

With the explosive growth in online commerce, more people are making online purchases with credit cards, which requires people to provide their private data to e-commerce websites; therefore, consumers should be careful to protect their personal identity and private data. Moreover, laws require organizations to use security controls to protect individuals'

private data. A **security control** is a safeguard or countermeasure an organization implements to help reduce risk. Examples of such controls include the following:

- Conducting annual security awareness training for employees, which helps remind staff about proper handling of private data and drives awareness of the organization's framework of security policies, standards, procedures, and guidelines.
- Implementing an IT security policy framework, which is 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. Through performing these tasks, security professionals verify that they have properly installed the controls.
- Enabling security incident and event monitoring at the Internet entry and exit points, which is like using a microscope to see what is coming in and going out.
- Using automated workstation and server antivirus and malicious software protection, which helps to keep viruses and malicious software out of computers.
- Using more stringent access controls beyond a logon ID and password for sensitive systems, applications, and data. Access to more sensitive systems should have a second test to confirm the user's identity.
- Minimizing software weaknesses in computers and servers by updating them with patches and security fixes, which helps to keep the 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, such as the following:

- Defining organization-wide policies, standards, procedures, and guidelines to protect confidential data, all of which provide guidance for how to handle private data.
- Adopting a **data classification standard** that defines how to treat data throughout the IT infrastructure, which 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.
- Using cryptography techniques to hide confidential data and keep it inaccessible to unauthorized users.
- Encrypting data that crosses the public Internet.
- Encrypting data that is stored within databases and storage devices.

Sending data to other computers, using a network, means that confidential data must be kept from unauthorized users, which entails the use of cryptography to make it unreadable. Thus, encryption is the process of transforming data from cleartext (i.e., data that anyone can read) into ciphertext (i.e., the scrambled data that results from encrypting cleartext). An example of this process is shown in **FIGURE 1-7**.

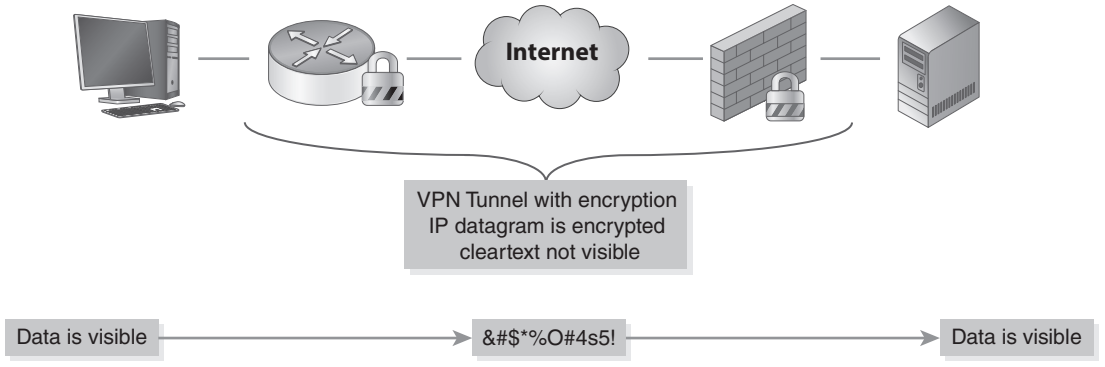


FIGURE 1-7
Encryption of cleartext into ciphertext.

Data confidentiality and privacy are so important that local and state governments are passing and strengthening laws to protect it at the state and federal levels.

Integrity

Integrity deals with the validity and accuracy of data. Data lacking integrity—that is, data that is not accurate nor valid—is of no use. For some organizations, data and information are intellectual property assets, examples of which include copyrights, patents, secret formulas, and customer databases. This information can have great value, which unauthorized changes can undermine. For this reason, integrity is a tenet of systems security. **FIGURE 1-8** shows what is meant by data integrity and whether that data is usable. Sabotage and corruption of data integrity are serious threats to an organization, especially if the data is critical to business operations.

⚠ WARNING

Because email traffic transmits through the Internet in cleartext, which means it is completely visible to whomever sees the email, never enter private data in an email. Moreover, never enter private data in a website if that site is not a trusted host, which can be checked by telephone or other means, nor into a website or web application that does not use encryption (e.g., look for the lock icon in the computer's browser to verify whether **Hypertext Transfer Protocol Secure (HTTPS)** encryption is enabled on that website or application).

Availability

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

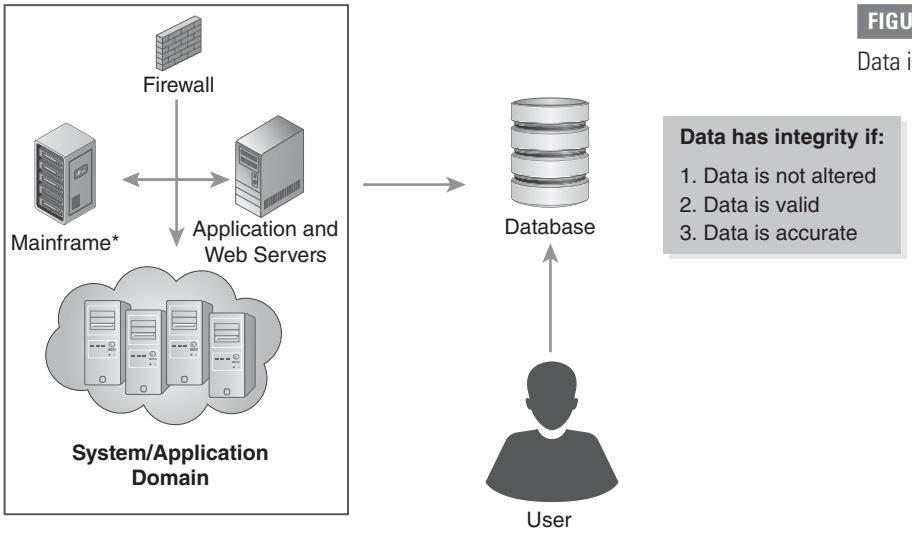


FIGURE 1-8
Data integrity.

- **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, therefore, have an MTTF of many years (25 or more). 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 point objective (RPO)**—RPO is the amount of data that an organization can lose and still operate. A successful recovery operation recovers data such that the net loss is smaller than the RPO.
- **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. BCPs 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)

the availability factor for a 30-day calendar month with 30 minutes of scheduled downtime in that calendar month is calculated 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 99.93 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.

Each domain requires proper security controls, which must meet the requirements of the C-I-A triad. Following is an overview of the seven domains and the risks, threats, and vulnerabilities commonly found in today's IT environments. Each domain may not be represented in every IT environment you encounter, but the infrastructure provides a good framework for discussing a strong, layered approach to security.

User Domain

The User Domain defines the people and processes that access an organization's information system.

User Domain Roles, Responsibilities, and Accountability

Following is an overview of what should go on in the User Domain:

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

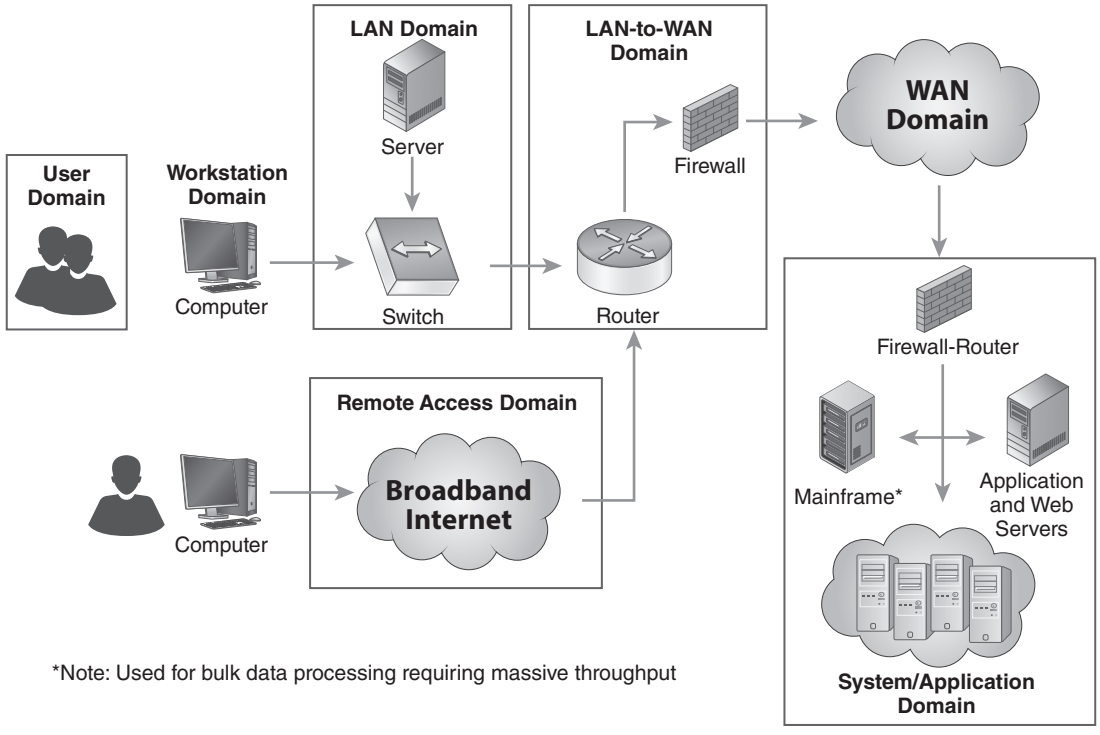


FIGURE 1-9

The seven domains of a typical IT infrastructure.

An acceptable use policy (AUP), which is like a rule book for employees that defines what they are allowed and not allowed to do with organization-owned IT assets, will be found in this domain. Violation of these rules can be grounds for dismissal.

- **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, and some organizations require a criminal background check for sensitive positions. The department 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, which 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. This domain is where the first layer of defense starts for a layered security strategy. **TABLE 1-2** lists the risks and threats commonly found in this 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 AUP, 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 CD/DVDs and USB drives with personal photos, music, and videos	Disable internal CD/DVD 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 a 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

The Workstation Domain includes all the workstations where the production of an organization takes place. A **workstation** can be any device that connects to the network, such as desktop or laptop computers, smartphones, tablets, and other lightweight computers (e.g., Chromebooks and Raspberry Pi computers). More details about mobile devices can be found in the "Remote Access Domain" section of this chapter.

Moreover, a workstation computer can be either a thin or a thick client. A true **thin client** can refer to a 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. More commonly, regular computers with normal hard drives are used as thin clients such that most of the "real" work occurs on a server or in the cloud. Thin clients are commonly used in large organizations, libraries, and schools. In contrast, a **thick client** has more fully featured hardware that contains a hard drive and applications and processes data locally, going to the server or cloud mainly for file storage.

Workstation Domain Roles, Responsibilities, and Accountability

Following is 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, and it includes activities such as 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 domain's entry into the IT infrastructure.
- **Responsibilities**—An organization's desktop support group is responsible for the Workstation Domain, including enforcing defined standards, which is critical to ensuring the integrity of user workstations and data. Typically, the human resources department defines proper access controls for workers based on their jobs, and IT security personnel then assign access rights to systems, applications, and data based on this definition. Moreover, the IT security personnel must safeguard controls within the Workstation Domain.
- **Accountability**—An organization's IT desktop manager is typically accountable for allowing employees the greatest use of the Workstation Domain, and 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, through logon IDs and passwords, because this domain is where users first access systems, applications, and data. The Workstation Domain is where the second layer of defense is required. **TABLE 1-3** lists the risks, threats, and vulnerabilities commonly found in the Workstation Domain along with ways to protect against them.

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 administration 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-factor authentication).
Desktop or laptop computer operating system software vulnerabilities	Define a workstation operating system **vulnerability window** policy and standard. The vulnerability window is the time from when a workstation is exposed to a known vulnerability until it is 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/DVDs or 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 want to use their own smartphones 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 other mobile devices. Typically, BYOD policies and procedures permit the organization to data wipe the employee's smartphone or mobile device if it is lost or the employee is terminated.

LAN Domain

The third component in the IT infrastructure is the LAN Domain. A **local area network (LAN)** is a collection of computers and devices connected to one another or to a common connection medium, which can include wires, fiber-optic cables, or radio waves. LANs are generally organized by function or department, and users get access to their department's LAN and other applications according to what their job requires. Once connected, computers can access systems, applications, and data and possibly the Internet.

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

- **Network interface controller (NIC)**—The **network interface controller (NIC)** is 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 10/100/1,000 Mbps Ethernet networking. **Ethernet** is the most popular LAN standard and is based on 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 (UTP) cabling**—This workstation cabling uses RJ-45 connectors and jacks to physically connect to a 100-Mbps/1-Gbps/10-Gbps Ethernet LAN switch. Today, organizations use Category 5 or 6 UTP transmission media to support high-speed data communications.
- **LAN switch**—A device that connects workstations into a physical Ethernet LAN. A switch provides dedicated Ethernet LAN connectivity for workstations and servers to deliver maximum throughput and performance for each workstation. There are two kinds of LAN switches. 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**—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 so that mobile laptops can connect. The WAP connects back to the LAN switch using UTP 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 (i.e., 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 configuration involves, for example, IP addressing, the **IP default gateway router**, and subnet mask address. The IP default gateway router acts as the entry and 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 is 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 **virtual LAN (VLAN)**, even though they may be connected to different physically connected LANs, which is the same thing as configuring workstations and servers to be on the same Ethernet LAN or broadcast domain.

LAN Domain Roles, Responsibilities, and Accountability

Following is 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
  - WAPs

  LAN system administration includes maintaining the master lists of user accounts and access rights. In this domain, two-factor authentication might be required. Two-factor authentication is like a gate whereby users must confirm their identity a second time, which mitigates the risk of unauthorized physical access.
- **Responsibilities**—The LAN support group is in charge of the LAN Domain, which includes both the physical components 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 needs strong security and access controls. Users can access company-wide systems, applications, and data from this domain, which is where the third layer of defense is required to protect the IT infrastructure as well as the domain itself. **TABLE 1-4** lists the risks, threats, and vulnerabilities commonly found in the LAN Domain along with appropriate risk-reducing strategies.

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, and delete privileges on specific documents as needed.
LAN server operating system software vulnerabilities	Define server, desktop, and 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 software patches and fixes are uploaded.
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 before 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.

LAN-to-WAN Domain

The LAN-to-WAN Domain is where the IT infrastructure links to a WAN and the Internet. Unfortunately, connecting to the Internet is like rolling out the red carpet for bad actors. The Internet is open, public, and easily accessible by anyone, and most Internet traffic is cleartext, which 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, which is like advertising to the world what is being transmitted.

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 protocol 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, and it 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.xhtml.*

Because the TCP/IP suite of protocols lacks security, the need is greater for security controls in dealing with protocols in this family.

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

Following is 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 and is one of the most complex areas to secure within an IT infrastructure. Security must be maintained while also giving users as much access as possible, physical parts need to be managed to give easy access to the service, and the security appliances must be logically configured to adhere to policy definitions.

  Ensuring that these items are adhered to 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**—A network device used to transport IP packets to and from the Internet or WAN. IP packets are forwarded based on path determination decisions. Configuration tasks include IP routing and access control lists (ACLs), which, like a filter, 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.

- **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, proxy, 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; 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 server**—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 it is 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 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)**—SIEM 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 and includes both the physical components and logical elements. Group members are responsible for applying the defined security controls.
- **Accountability**—An organization's WAN network manager has a duty to manage the LAN-to-WAN Domain. Typically, the director of IT security ensures that this domain's 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 travels 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, which is also known as the Internet ingress and 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.

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 immediately if malicious.
Denial of service (DoS)/distributed denial of service (DDoS) attacks on external public-facing IPs and Internet links	Upstream Internet service providers (ISPs) must participate in DoS/DDoS attack prevention and discarding of IP packets when a stream of half-open TCP synchronize (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 ACLs. 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 Uniform Resource Locator (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 and access point.

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.
- **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 24/7/365.
- **Service-level agreements (SLAs)**—Contractual commitments for monthly service offerings, such as availability, packet loss, and response time to fix problems.

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

Following is 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 and is the second most complex area to secure within an IT infrastructure. The goal is to allow users the most access possible while making sure that 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 links are the physical communication links provided as a digital or optical service terminated at a company's 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
    - 10/100/1,000 Mbps metro Ethernet LAN connectivity, depending on physical distance
  - **IP network design**—This is the logical design of the IP network and addressing schema and 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 stand-alone 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 **virtual private network (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. It is a form of the Layer 1/Layer 3 overlay network and bypasses the routing function's path determination process once a long-lived flow has been 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. These responsibilities include both the physical components and logical elements. Network engineers and security practitioners set up 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**—An 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 and are responsible for securing their network infrastructure. Customers who sign up for WAN communication services must review the terms, conditions, and limitations of liability within their service contract to determine where the service provider's duties start and end regarding router 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 represents the fifth layer of security for an overall IT infrastructure. **TABLE 1-6** lists the risks, threats, and vulnerabilities found in the Internet segment of the WAN Domain and appropriate risk-reducing strategies.

Besides selling WAN connectivity services, some telecommunications service providers now also provide security management services. The following section presents WAN connectivity risks, threats, and vulnerabilities and risk-reducing 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 AUPs 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, specifically follow its policies, procedures, and guidelines.
Vulnerable to eavesdropping	Use encryption and VPN tunnels for end-to-end secure IP communications. If you have a data classification standard, specifically follow its 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 the ISP to put the proper filters on its IP router WAN interfaces in accordance with CERT Advisory CA-1996-21, which can be found here: *https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=496170*.
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 (e.g., HTTP, FTP, and TFTP)	Refer to the 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.
Hackers, attackers, and perpetrators email Trojans, worms, and malicious software	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 has been 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.

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

Telecommunications companies are responsible for building and transporting customer IP traffic, which sometimes is bundled with dedicated Internet access to provide shared broadband access organization-wide. If organizations outsource their WAN infrastructure, management and security must extend to the service provider. Therefore, organizations