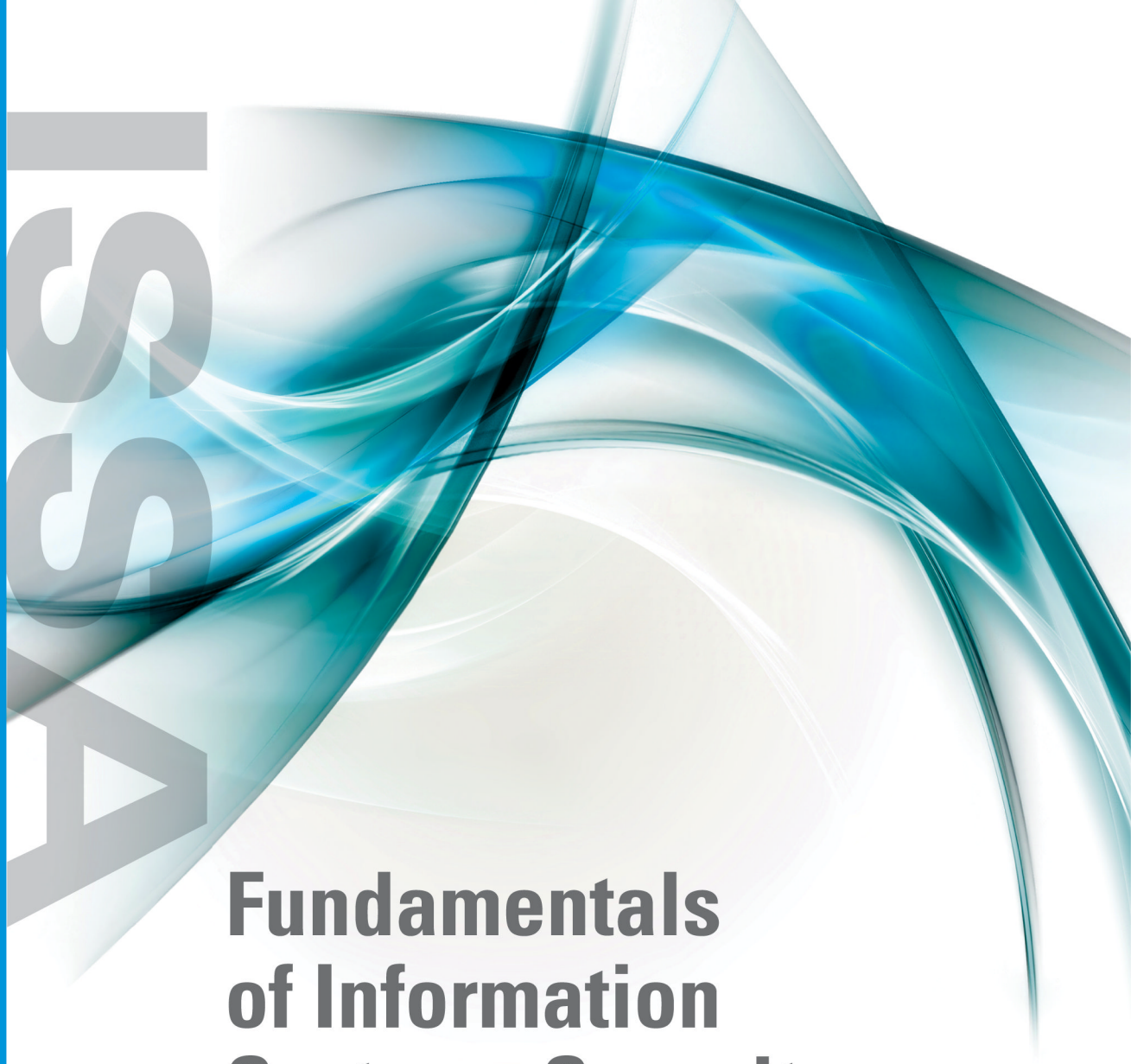


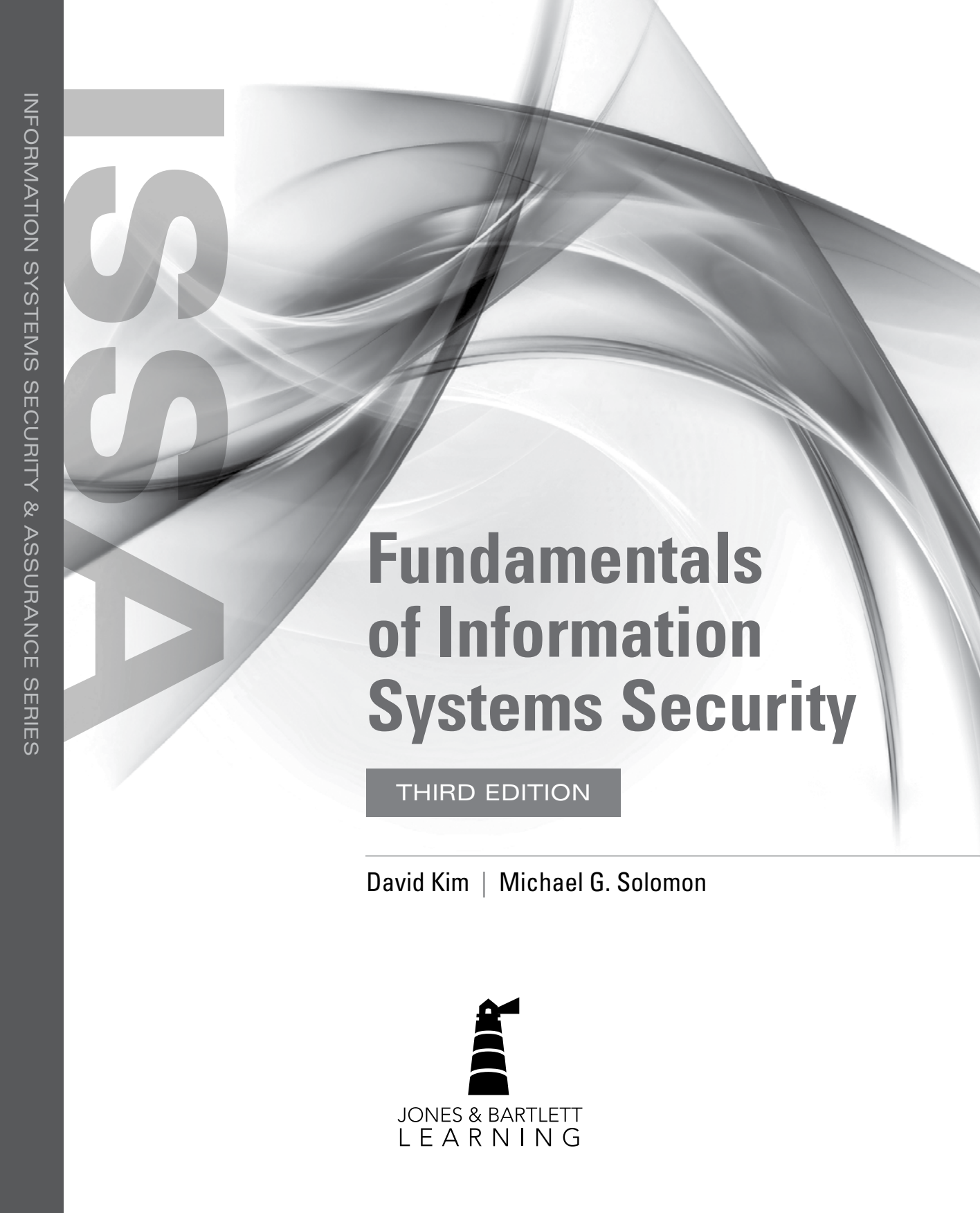
INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES

ISSA

Fundamentals of Information Systems Security

THIRD EDITION

David Kim | Michael G. Solomon



Fundamentals of Information Systems Security

THIRD EDITION

David Kim | Michael G. Solomon

JONES & BARTLETT
LEARNING

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

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

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

Production Credits
VP, Executive Publisher: David D. Cella
Executive Editor: Matt Kane
Acquisitions Editor: Laura Pagluica
Editorial Assistant: Mary Menzemer
Production Manager: Carolyn Rogers Pershouse
Associate Production Editor: Juna Abrams
Director of Marketing: Andrea DeFronzo
Marketing Manager: Amy Langlais
Manufacturing and Inventory Control Supervisor: Amy Bacus
Composition: S4Carlisle Publishing Services
Cover Design: Scott Moden
Director of Rights & Media: Joanna Gallant
Rights & Media Specialist: Merideth Tumasz
Media Development Editor: Shannon Sheehan
Cover and Header Image: © Zffoto/Shutterstock
Printing and Binding: Edwards Brothers Malloy
Cover Printing: Edwards Brothers Malloy

Library of Congress Cataloging-in-Publication Data
Names: Kim, David (Information technology security consultant), author. |
Solomon, Michael (Michael G.), 1963- author.
Title: Fundamentals of information systems security / David Kim and Michael G. Solomon.
Description: Third edition. | Burlington, Massachusetts : Jones & Bartlett
Learning, 2016. | Includes bibliographical references and index.
Identifiers: LCCN 2016038356 | ISBN 9781284116458 (pbk.)
Subjects: LCSH: Computer security. | Information resources--Security measures.
Classification: LCC QA76.9.A25 K536 2016 | DDC 005.8--dc23
LC record available at https://lccn.loc.gov/2016038356

6048

Printed in the United States of America
20 19 18 17 16 10 9 8 7 6 5 4 3 2 1

This book is dedicated to our readers, students, and 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 privacy 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 Book

This book 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, they deliver comprehensive information on all aspects of information security. Reviewed word for word by leading technical experts in the field, these books are not just current, but forward-thinking—putting you in the position to solve the cybersecurity challenges not just of today, but of tomorrow, as well.

Part I of this book 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 book 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.

Learning Features

The writing style of this book is practical and conversational. Step-by-step examples of information security concepts and procedures are presented throughout the text. Each chapter begins with a statement of learning objectives. Illustrations are used both to clarify the material and to 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 book.

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

Audience

The material is suitable for undergraduate or graduate computer science majors or information science majors, students at a 2-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

This is the flagship book of the Information Systems Security & Assurance (ISSA) Series from Jones & Bartlett Learning (*www.issaseries.com*). The ISSA series was designed for IT security and information assurance curriculums and courseware for those colleges and universities needing a hands-on approach to delivering an information systems security and information assurance degree program whose graduates would be ready for the work force.

The entire ISSA series was developed by information systems security professionals, consultants, and recognized leaders in the field of information systems security, all of whom contributed to each word, sentence, paragraph, and chapter. The dedication and perseverance displayed by those involved was driven by a single passion and a common goal: "to help educate today's information systems security practitioner" by creating the most up-to-date textbooks, courseware, and hands-on labs to ensure job and skill-set readiness for information systems security practitioners.

Thank you to Jones & Bartlett Learning for having the vision and patience to champion this effort and build the world's best information systems security content and curriculum. Thank you to Michael Solomon and Jeff Parker and the entire Jones & Bartlett Learning team who contributed to this book and entire ISSA Series during the past 6 months of development.

And last but not least, I would like to thank my wife, MiYoung Kim, who is and always will be by my side. I love you more each day.

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. And thanks so much to Stacey and Noah for your help in researching the many diverse topics.

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 healthcare 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, CISSP, PMP, CISM, is a full-time security and OpenEdge speaker, consultant, author, and gamification evangelist who specializes in leading teams in achieving and maintaining secure IT environments. As an IT professional and consultant since 1987, he has led projects for many major organizations and has authored and contributed to numerous books and training courses. From 1998 until 2001, he was an instructor in the Kennesaw State University's Computer Science and Information Sciences (CSIS) department, and currently teaches graduate Computer Science and Security courses at the University of the Cumberlands. Michael is also a PhD candidate in Computer Science and Informatics at Emory University.

PART I

The Need for Information Security

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

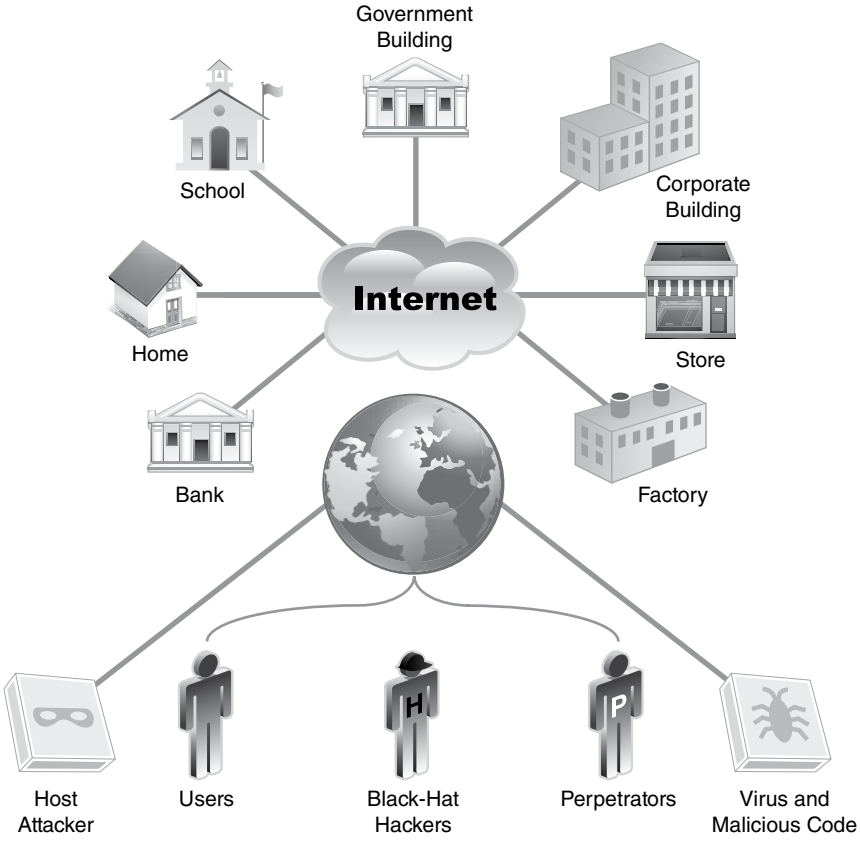


FIGURE 1-1
Cyberspace: the new frontier.

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.