Cengage

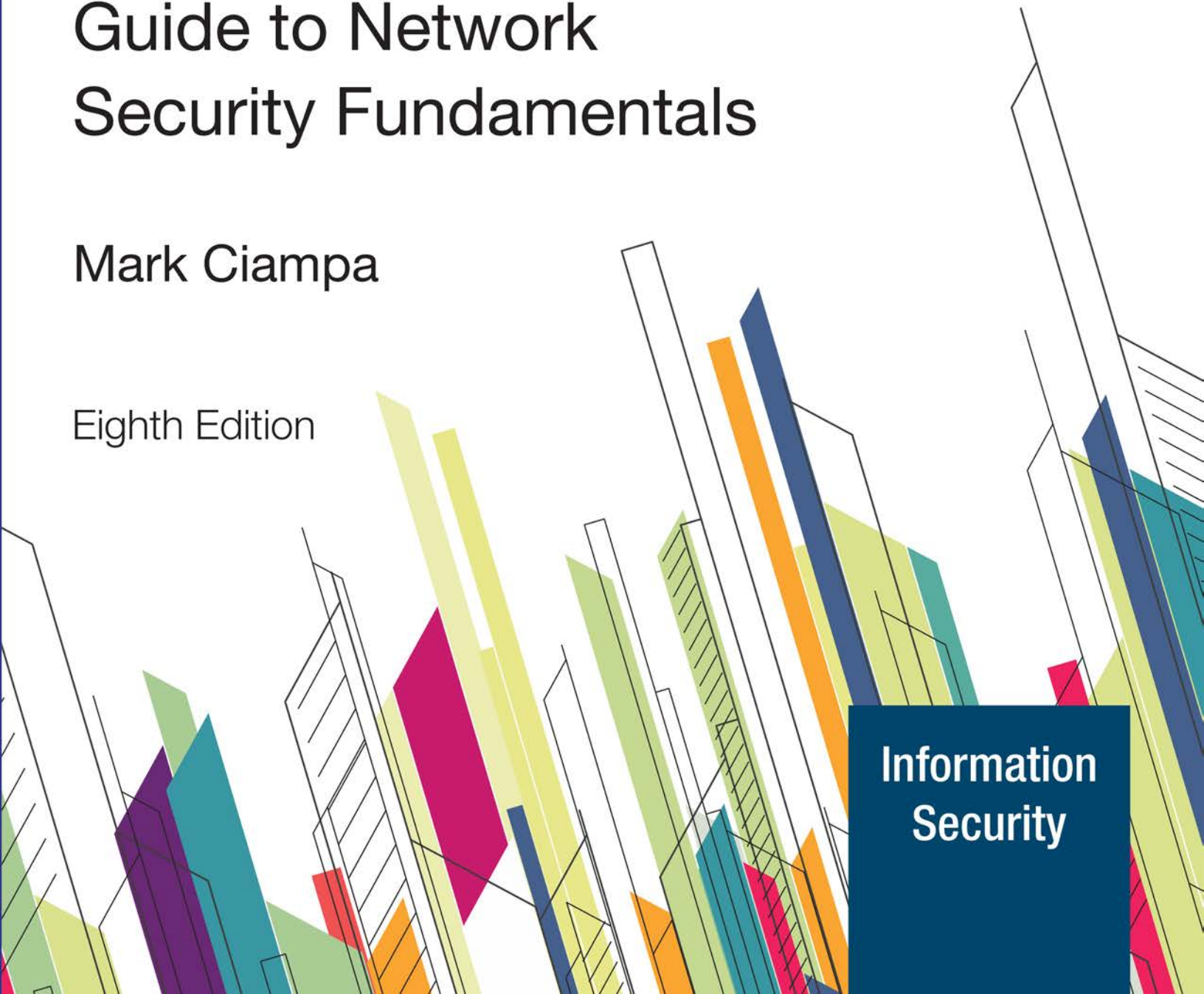
CompTIA

CompTIA Security+

Guide to Network Security Fundamentals

Mark Ciampa

Eighth Edition



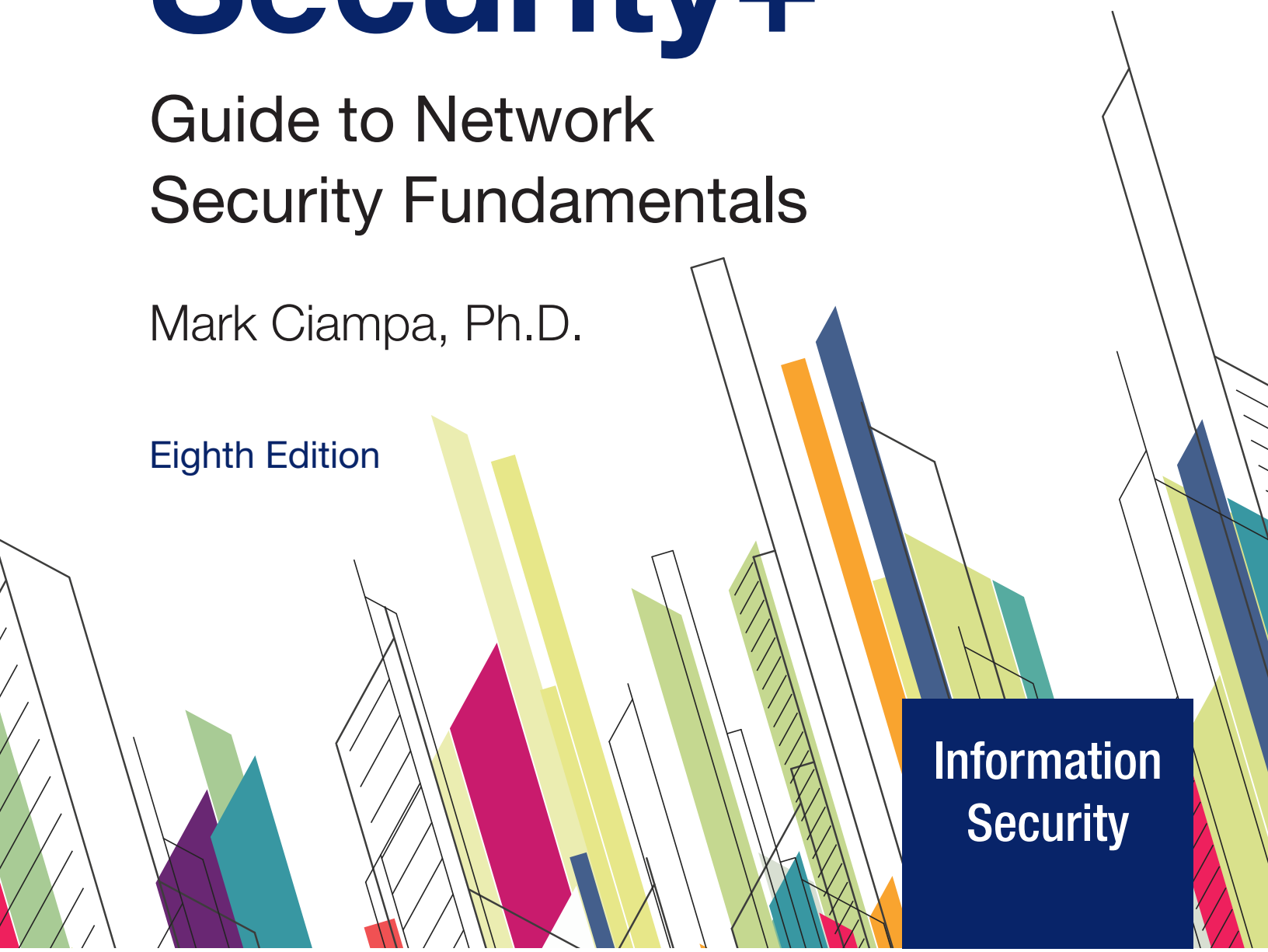
CompTIA

CompTIA® Security+

Guide to Network Security Fundamentals

Mark Ciampa, Ph.D.

Eighth Edition



Cengage

Australia • Brazil • Canada • Mexico • Singapore • United Kingdom • United States

Cengage

***CompTIA Security+ Guide to Network Security Fundamentals*, Eighth Edition**
Mark Ciampa

SVP, Product: Cheryl Costantini

VP, Product: Thais Alencar

Senior Product Director, Portfolio Product Management: Mark Santee

Director, Product Management: Rita Lombard

Portfolio Product Manager: Natalie Onderdonk

Product Assistant: Anh Nguyen

Learning Designer: Carolyn Mako

Senior Content Manager: Brooke Greenhouse

Digital Project Manager: Jim Vaughey

Technical Editor: Danielle Shaw

Developmental Editor: Lisa Ruffolo

VP, Product Marketing: Jason Sakos

Director, Product Marketing: Danae April

Product Marketing Manager: Mackenzie Paine

Portfolio Specialist: Matt Schiesl

Content Acquisition Analyst: Callum Panno

Production Service: Straive

Senior Designer: Erin Griffin

Cover Image Source: shuoshu/DigitalVision Vectors/Getty Images

Previous edition(s): © 2022, © 2018, © 2015
WCN: 02-300

Library of Congress Control Number: 2023916394

ISBN: 979-8-21-400063-3
Looseleaf: ISBN: 979-8-21-400064-0

Cengage
5191 Natorp Boulevard
Mason, OH 45040
USA

Cengage is a leading provider of customized learning solutions. Our employees reside in nearly 40 different countries and serve digital learners in 165 countries around the world. Find your local representative at **www.cengage.com**.

To learn more about Cengage platforms and services, register or access your online learning solution, or purchase materials for your course, visit **www.cengage.com**.

Notice to the Reader
Publisher does not warrant or guarantee any of the products described herein or perform any independent analysis in connection with any of the product information contained herein. Publisher does not assume, and expressly disclaims, any obligation to obtain and include information other than that provided to it by the manufacturer. The reader is expressly warned to consider and adopt all safety precautions that might be indicated by the activities described herein and to avoid all potential hazards. By following the instructions contained herein, the reader willingly assumes all risks in connection with such instructions. The publisher makes no representations or warranties of any kind, including but not limited to, the warranties of fitness for particular purpose or merchantability, nor are any such representations implied with respect to the material set forth herein, and the publisher takes no responsibility with respect to such material. The publisher shall not be liable for any special, consequential, or exemplary damages resulting, in whole or part, from the readers' use of, or reliance upon, this material.

Printed in the United States of America
Print Number: 01 Print Year: 2023

Brief Contents

Table of Contents

Part 2

Module 3

Module 4

Part 3

Module 5

Module 6

Module 7

Part 4

Module 8

Module 9

Module 13

Module 14

Module 15

Appendix A

Introduction

Astronomical, *enormous*, *humongous*—these are all words to describe the impact and scope of cyberattacks today. A security operations center at a port authority reports that they receive 40 million attempted cyberattacks each *month*. The total number of instances of malware has grown from 182 million in 2013 to over 1.34 billion today. Cybercrime has been called the "greatest transfer of economic wealth in history," and it is estimated that it could reach $10.5 trillion *annually* by 2025. And the recent introduction of artificial intelligence (AI) tools has only heightened cybersecurity attacks. A 135 percent increase in phishing and spam emails has been directly linked to AI. Two security researchers used an AI tool to win a "hack-a-thon" contest, earning them a prize of $123,000. The extent to which AI tools will assist attackers to launch hard-to-detect attacks is frightening.

The need to identify and defend against around-the-clock cyberattacks that target all businesses large and small has created an essential workforce that is now at the very core of the information technology (IT) industry. Known as information security, these professionals are focused on protecting electronic information. The demand for these certified professionals in information security has never been higher. However, a large gap remains. Although the global cybersecurity workforce grew to 4.7 million workers in 2021, reaching its highest-ever levels, there is still a need for more than *3.4 million* security professionals, an increase of over 26 percent from the prior year.

When filling cybersecurity positions, an overwhelming majority of enterprises use the Computing Technology Industry Association (CompTIA) Security+ certification to verify security competency. Of the hundreds of security certifications currently available, Security+ is one of the most widely acclaimed security certifications. Because it is internationally recognized as validating a foundation level of security skills and knowledge, the Security+ certification has become the foundation for today's IT security professionals. The value for an IT professional who holds a CompTIA security certification is significant. On average, an employee with a CompTIA certification commands a salary between 5 and 15 percent higher than their counterparts with similar qualifications but lacking a certification.

The CompTIA Security+ certification is a vendor-neutral credential that requires passing the current certification exam SY0-701. A successful candidate has the knowledge and skills required to identify attacks, threats, and vulnerabilities; design a strong security architecture; implement security controls; be knowledgeable of security operations and incident response; and be well versed in governance, risk, and compliance requirements.

Certification provides job applicants with more than just a competitive edge over their noncertified counterparts competing for the same IT positions. Some institutions of higher education grant college credit to students who successfully pass certification exams, moving them further along in their degree programs. For those already employed, achieving a new certification increases job effectiveness, which opens doors for advancement and job security. Certification also gives individuals who are interested in careers in the military the ability to move into higher positions more quickly.

CompTIA® Security+ Guide to Network Security Fundamentals, Eighth Edition, is intended to equip learners with the knowledge and skills needed to be information security IT professionals. Yet it is more than an "exam prep" book. While teaching the fundamentals of information security by using the CompTIA Security+ exam objectives as its framework, the book takes a comprehensive view of security by examining in depth today's attacks against networks and endpoints and what is needed to defend against these attacks. This book is a valuable tool for those who want to learn about information security and enter the field. It also provides the foundation that will help prepare for the CompTIA Security+ certification exam. For more information on CompTIA Security+ certification, visit CompTIA's website at comptia.org.

Intended Audience

This book is designed to meet the needs of students and professionals who want to master basic information security. A fundamental knowledge of computers and networks is all that is required to use this book. Those seeking to pass the CompTIA Security+ certification exam will find the text's approach and content especially helpful; all Security+ SY0-71 exam objectives are covered in the text (see Appendix A). *Security+ Guide to Network Security Fundamentals, Eighth Edition*, covers all aspects of network and computer security while satisfying the Security+ objectives.

The book's pedagogical features are designed to provide a truly interactive learning experience to help prepare you for the challenges of network and computer security. In addition to the information presented in the text, each module includes Hands-On Projects that guide you through implementing practical hardware, software, network, and Internet security configurations step by step. Each module also contains case studies that place you in the role of problem solver, requiring you to apply concepts presented in the module to achieve successful solutions.

Module Descriptions

The following list summarizes the topics covered in each module of this course:

Module 1: Introduction to Information Security introduces the cybersecurity fundamentals that form the basis of the Security+ certification. The module begins by defining information security and identifying attackers. It also looks at how attacks occur and various information security resources.

Module 2: Pervasive Attack Surfaces and Controls looks at three topics—social engineering, physical security, and data controls—considered as "pervasive" since they apply universally across IT security.

Module 3: Fundamentals of Cryptography explores what cryptography is and how it is used along with cryptographic limitations and attacks on cryptography.

Module 4: Advanced Cryptography looks at the advanced features of cryptography, such as authentication and distribution of public keys through digital certificates, the management of keys through public key infrastructure, and different secure communication and transport protocols.

Module 5: Endpoint Vulnerabilities, Attacks, and Defenses examines vulnerabilities in applications and malware attacks on endpoints along with the defense measures that can be taken to mitigate these attacks.

Module 6: Mobile and Embedded Device Security explores mobile, embedded, and specialized device security by looking at securing mobile devices and Internet of Things devices along with how application software that runs on these and other devices can be securely designed and coded.

Module 7: Identity and Access Management (IAM) looks at how devices can be accessed by authorized users and restricting what users can do on the devices. It examines the different types of authentication credentials that can be used to verify a user's identity, best practices for authentication, and how to limit privileges through access controls.

Module 8: Infrastructure Threats and Security Monitoring begins a study of attacks and defenses of enterprise-level infrastructures and architectures by exploring common attacks that are launched against networks and tools for monitoring network security, and raising alerts when that security is compromised.

Module 9: Infrastructure Security investigates how to build a secure infrastructure through network security appliances and security software, network design, and access technologies.

Module 10: Wireless Network Attacks and Defenses explores wireless network security. It examines the attacks on wireless devices that are common today, then explores vulnerabilities in wireless security, and finally examines several secure wireless protections.

Module 11: Cloud and Virtualization Security looks at cloud computing and virtualization: what these technologies are, how they function, and how they can be secured.

Module 12: Vulnerability Management examines the security vulnerability management process by looking at running a vulnerability scan and how to address the results along with different types of audits and assessments, particularly penetration testing.

Module 13: Incident Preparation and Investigation focuses on the plans that must be made for when a cyber incident occurs. These plans cover incident preparation, building resilience through redundancy, and follow-up investigations as to how an incident occurred and how similar future events can be mitigated.

Module 14: Oversight and Operations explores administration principles such as governance and compliance and also looks at security operations: automation, orchestration, and threat hunting. It also examines the impact of AI on information security.

Module 15: Information Security Management examines five key information security management processes: asset management, risk management, third-party risk management, change management, and awareness management.

Appendix A: CompTIA SY0-701 Certification Examination Objectives provides a complete listing of the latest CompTIA Security+ certification exam objectives and shows the modules and headings in the modules that cover material associated with each objective, as well as the Bloom's Taxonomy level of that coverage.

Features

The course's pedagogical features are designed to provide a truly interactive learning experience and prepare you to face the challenges of cybersecurity. To aid you in fully understanding computer and network security, this course includes many features designed to enhance your learning experience.

- **Maps to CompTIA Objectives.** The material in this text covers all the CompTIA Security+ SY0-701 exam objectives.
- **Module Objectives.** Each module lists the concepts to master within that module. This list serves as a quick reference to the module's contents and as a useful study aid.
- **#TrendingCyber.** This section opens each module and provides an explanation and analysis of some of the latest attacks and defenses related to topics that are covered in the module. The sections establish a real-world context for understanding information security.
- **Illustrations, Tables, and Bulleted Lists.** Numerous full-color diagrams illustrating abstract ideas and screenshots of cybersecurity tools help learners better visualize the concepts of cybersecurity. In addition, the many tables and bulleted lists provide details and comparisons of both practical and theoretical information that can be easily reviewed and referenced in the future.
- **Summary.** Each module reading concludes with a summary of the concepts introduced in that module. These summaries revisit the ideas covered in each module.
- **Key Terms.** All of the terms in each module that were introduced with blue text are gathered in a Key Terms list, providing additional review and highlighting key concepts. Key term definitions are included in the Glossary at the end of the text.
- **Review Questions.** The end-of-module assessment begins with a set of review questions that reinforce the ideas introduced in each module. These questions help you evaluate and apply the material you have learned. Answering these questions will ensure that you have mastered the important concepts and provide valuable practice for taking CompTIA's Security+ exam.
- **Hands-On Projects.** Projects at the end of each module give you the opportunity to apply in practice what you have just learned. These projects include detailed step-by-step instructions to walk you through endpoint security configuration settings and demonstrate actual security defenses using websites or software downloaded from the Internet. In addition, instructions are provided regarding how to perform these projects in a protected sandbox environment so that the underlying computer is not impacted.
- **Case Projects.** Although it is important to understand the theory behind information security technology, nothing beats real-world experience. To this end, each module includes several case projects aimed at providing practical implementation experience as well as practice in applying critical thinking skills to reinforce the concepts learned throughout the module.

New to This Edition

- Maps fully to the latest CompTIA Security+ exam SY0-701
- Completely revised and updated with expanded coverage on attacks and defenses
- New module units: Security Foundations, Cryptography, Device Security, Infrastructure and Architectures, and Operations and Management
- All new "#TrendingCyber" opener in each module

- All new Two Rights & a Wrong self-assessments that give you opportunities to quickly assess your understanding of the topics
- All new live virtual machine labs that help you refine the hands-on skills needed to master today's cybersecurity toolset
- New and updated Hands-On Projects cover some of the latest security software
- Expanded and new Case Projects that provide opportunities to explore topics in greater depth
- All new introductions to the Hands-On Projects and Case Projects provide time estimates, objectives, and project descriptions
- New cybersecurity consultant and assurance service scenarios in which you serve as an intern and gain practical experience regarding what you might encounter on the job
- All SY0-701 exam topics fully defined
- Linking of each exam subdomain to Bloom's Taxonomy (see Appendix A)

Text and Graphic Conventions

Wherever appropriate, additional information and exercises have been added to this book to help you better understand the topic at hand. Icons throughout the text alert you to additional materials. The following icons and elements are used in this textbook:

Note 1

Numbered Note elements draw your attention to additional helpful material related to the subject being described.

Caution !

The Caution icons warn you about potential mistakes or problems and explain how to avoid them.

Two Rights & A Wrong

The "Two Rights & a Wrong" elements let you quickly assess your understanding of the topics. The answers to these assessments appear at the end of each module.

Virtual Labs The VM Lab icons alert you to live, virtual machine labs that reinforce the material in each module.

Certification

Certification icons indicate CompTIA Security+ objectives covered under major module headings.

Instructor's Materials

Instructors, please visit cengage.com and sign in to access instructor-specific resources, which include the Instructor's Manual, Solution and Answer Guide, Instructor Test Banks, and PowerPoint presentations.

- **Instructor's Manual.** The Instructor's Manual that accompanies this text provides additional instructional material to assist in class preparation, including suggestions for discussion topics and additional projects.
- **Solution and Answer Guide.** The instructor's resources include solutions to all end-of-module material, including review questions, hands-on projects, and case projects.
- **Cengage Testing Powered by Cognero.** This flexible, online system allows you to do the following:
  - Author, edit, and manage test bank content from multiple Cengage solutions.
  - Create multiple test versions in an instant.
  - Deliver tests from your learning management system, your classroom, or wherever you want.
- **PowerPoint Presentations.** This course comes with Microsoft PowerPoint slides for each module. These slides are meant to be used as a teaching aid for classroom presentations, to make available to students on the network for module review, or to be printed for classroom distribution. Instructors can add their own slides for additional topics introduced to the class.

MindTap

MindTap for *Security+ Guide to Network Security Fundamentals, Eighth Edition*, is an online learning solution designed to help you master the skills needed in today's workforce. Research shows that employers need critical thinkers, troubleshooters, and creative problem-solvers to stay relevant in our fast-paced, technology-driven world. MindTap helps you achieve this with assignments and activities that provide hands-on practice, real-life relevance, and proficiency in difficult concepts. Students are guided through assignments that progress from basic knowledge and understanding to more challenging problems. MindTap activities and assignments are tied to learning objectives. MindTap features include the following:

Live Virtual Machine Labs allow you to practice, explore, and try different solutions in a safe sandbox environment. Each module provides you with an opportunity to complete an in-depth project hosted in a live virtual machine environment. You implement the skills and knowledge gained in the module through real design and configuration scenarios.

Simulations allow you to apply concepts covered in the module in a step-by-step virtual environment. The simulations provide immediate feedback.

Security for Life assignments encourage you to stay current with what is happening in the field of cybersecurity.

Reflection activities encourage classroom and online discussion of key topics covered in the modules.

Pre- and Post-Assessments assess your understanding of key concepts at the beginning and end of the course and emulate the text.

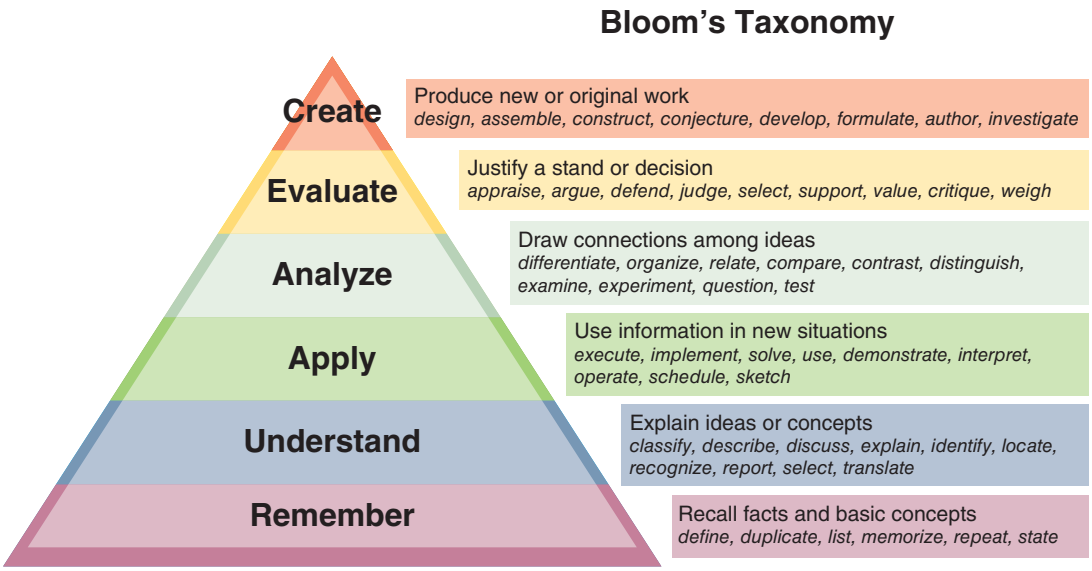
Lab Manual contains hands-on exercises that use fundamental networking security concepts as they are applied in the real world. Each module lab manual offers review questions to reinforce your proficiency in network security topics and to sharpen your critical thinking and problem-solving skills.

For instructors, MindTap is designed around learning objectives and provides analytics and reporting so you can easily see where the class stands in terms of progress, engagement, and completion rates. Use the content and learning path as is or pick and choose how your materials will integrate with the learning path. You control what the students see and when they see it. Learn more at www.cengage.com/mindtap/.

Instant Access Code: (9798214000664)

Printed Access Code: (9798214000671)

Figure A Bloom's taxonomy



What's New with CompTIA Security+ Certification

The CompTIA Security+ SY0-701 exam was updated in November 2023. Several significant changes have been made to the exam objectives. The exam objectives have been expanded to reflect current security issues and knowledge requirements more accurately. These exam objectives place importance on knowing "how to" rather than just knowing or recognizing security concepts.

Here are the domains covered on the new Security+ exam:

Domain	% of Examination
1.0 General Security Concepts	12%
2.0 Threats, Vulnerabilities, and Mitigations	22%
3.0 Security Architecture	18%
4.0 Security Operations	28%
5.0 Security Program Management and Oversight	20%
Total	100%

CompTIA

Your Next Move Starts Here!

Get CompTIA certified to help achieve your career goals and gain a powerful, vendor-neutral credential that is trusted by employers.

Save 10%
when you purchase your exam voucher from CompTIA.org.

Use code:
Cengage10

Why get CompTIA certified?

Increase your confidence
91% of certification earners show increased confidence.*

Earn more money
77% of IT pros got a raise within six months of earning their certification.*

Stand out to employers
64% of IT decision makers say certified employers add additional value.**

Join a global community
92% of IT professionals hold at least one certification.**

Get ready for exam day.

- **Download the exam objectives:** Visit CompTIA.org to find the exam objectives for your IT certification and print them out. This is your roadmap!
- **Create your study plan:** Decide how many hours each week you are going to dedicate to studying, choose your preferred study tools and get to work. Studying is a unique experience. Download a study plan worksheet on CompTIA.org.
- **Get certified:** If you haven't already, use the coupon on this page when you purchase your exam voucher and schedule your exam. CompTIA offers flexible testing options to fit your busy life.

Choose your testing option.

Online testing
Earn a CompTIA certification online, from your home – or any quiet, distraction-free, secure location – at a time that's convenient for you.

In-person testing
Test at any of the Pearson VUE test centers around the world, where you can use their equipment under the supervision of a proctor.

To purchase your exam voucher and learn how to prepare for exam day, visit CompTIA.org.

*Pearson VUE 2021 Value of IT Certifications
**2021 Global Knowledge IT Skills and Salary Report

About the Author

Dr. Mark Ciampa is Professor of Analytics and Information Systems and Program Director of the graduate Cybersecurity Data Analytics program in the Gordon Ford College of Business at Western Kentucky University in Bowling Green, Kentucky. Prior to this, he was an associate professor and served as the Director of Academic Computing at Volunteer State Community College in Gallatin, Tennessee, for 20 years. Dr. Ciampa has worked in the IT industry as a computer consultant for businesses, government agencies, and educational institutions. He has published over 25 articles in peer-reviewed journals and books. He is also the author of over 30 technology textbooks from Cengage, including *CompTIA CySA+ Guide to Cybersecurity Analyst, Second Edition, CWNA Guide to Wireless LANs, Third Edition, Guide to Wireless Communications, Security Awareness: Applying Practical Cybersecurity in Your World, Sixth Edition,* and *Networking BASICS*. Dr. Ciampa holds a PhD in technology management with a specialization in digital communication systems from Indiana State University and has certifications in security and healthcare.

Acknowledgments

A large team of dedicated professionals all contributed to this project, and I am honored to be part of such an outstanding group. First, thanks go to Cengage Portfolio Product Manager Natalie Onderdonk for providing me with the opportunity to work on this project and for providing continual support. Thanks also to Senior Content Manager Brooke Greenhouse for answering all my questions, to Learning Designer Carolyn Mako for her helpful suggestions, and to Danielle Shaw for her technical reviews. And special recognition goes to developmental editor Lisa Ruffolo. From beginning to end Lisa was there to manage the details, provide me with innumerable helpful suggestions, and coordinate all the different activities so that I could focus on my work. It is truly a great pleasure to work with Lisa. I also appreciated the significant contributions of the reviewers for this edition: Bess Ann Gonyea, Ivy Tech Community College; Willis Holmes, Hopkins County Schools; and Dr. Seon A. Levius, State University of New York at Potsdam. To everyone on this team and at Cengage Learning, I extend my sincere thanks.

Finally, I want to thank my wonderful wife, Susan. Her continual patience, support, and love were always a great encouragement to me. I could not have done this project without her.

Dedication

To Braden, Mia, Abby, Gabe, Cora, Will, and Rowan

Before You Begin

This book should be read in sequence, from beginning to end. Each module builds on those that precede it to provide a solid understanding of networking security fundamentals. The book may also be used to prepare for CompTIA's Security+ certification exam. Appendix A pinpoints the modules and sections in which specific Security+ exam objectives are covered.

Hardware and Software Requirements

Following are the hardware and software requirements needed to perform the end-of-module Hands-On Projects.

- Microsoft Windows 11
- An Internet connection and web browser
- Microsoft Office

Free, Downloadable Software Requirements

Free, downloadable software is required for the Hands-On Projects in the following modules.

Module 3:
- OpenPuff Steganography
- 7-Zip

Module 4:
- Microsoft Root Certificates

Module 5:
- Microsoft Safety Scanner
- Refog Keylogger

Module 6:
- NoxPlayer

Module 7:
- KeePass

Module 8:
- Technitium MAC address changer

Module 9:
- GlassWire
- ProtonVPN

Module 10:
- WifiInfoView
- Vistumbler

Module 11:
- VirtualBox

Module 13:
- Directory Snoop

Module 14:
- Browzar

Part 1

Security Foundations

Unrelenting, *unyielding*, and *unstoppable* are the three words that may best describe today's cyberattacks. Everyone, ranging from a single user with a simple handheld device to massive multinational corporations with millions of employees, are all targets of attacks—and these attacks show no end in sight. The modules in Part 1 lay the foundations of information security by explaining what information security is, who is responsible for these attacks, and how they are being carried out.

Module 1
Introduction to Information Security

Module 2
Pervasive Attack Surfaces and Controls

Module 1

Introduction to Information Security

Module Objectives

After completing this module, you should be able to do the following:

1. Define information security and explain its principles
2. Identify threat actors and their motivations
3. Describe how attacks occur and the impact of attacks
4. List various information security resources

#TrendingCyber

A commonly held perception is that successful "hackers" will rarely face lengthy jail time or financial penalties if caught. Instead, they are offered lucrative careers in cybersecurity to protect the very systems that they once breached. However, this perception is false. As more attackers are caught and complete their prison sentences, they are finding it very difficult to land a job in cybersecurity or other technology fields.

Individuals convicted of certain crimes cannot always have the same privileges they once enjoyed prior to their arrest. In many states, convicted felons are not immediately eligible to vote in elections. Most states have other restrictions that impact people's employment once they are paroled from prison. For example, a former inmate who becomes a journalist may need additional approvals to ride along with police while researching a story, or they may not qualify for expedited screening like other journalists to enter a courthouse to cover a trial.

In a similar way, convicted cyberattackers in the United States and many European countries usually face restrictions on their use of computers and access to the Internet once they have served their sentence. The stated purpose of these restrictions is to prevent them from being in a position in which they would be tempted to reoffend. Restrictions for those convicted of a cybercrime typically require that their computers and technology devices must be registered with the court system, and they are prohibited from using any web applications or technologies that could mask their online behavior, such as virtual private networks. These restrictions can last up to 10 years after their release from prison.

Many former cybercriminals have reported that these restrictions on using technology have made it virtually impossible to find any job that uses technology at any level. One attacker was arrested and convicted for breaking into a telecom's system and exposing the personal data of 156,000 customers, costing the telecom $48 million. The attacker was only 18 years old when he committed the crime. After serving two years of a four-year sentence, he then faced three years of restrictions, which included a requirement to register any technology device he used and limited his access to apps and online services. Every few months authorities—without prior notice—seized his devices for inspection and made a copy of all his data. Another convicted cyberattacker applied for multiple tech jobs after being

released from prison, but the restrictions made it impossible to find a job. He was forced to work in construction and restaurants for several years until his probationary period expired.

A common step for entering the corporate workforce in information security is to earn a certificate in the field from a respected cyber organization. However, for most convicted cyberattackers, this too is a path that is unavailable to them. Many high-level certificates require the applicants to go through ethics and background checks before being certified. These certifications typically have ethics codes that require applicants to have acted "honorably, honestly, justly, responsibly, and legally." As the chief executive of one certification organization said, "It would be very unlikely we would allow them to hold our certification because of how closely tied that is to the violation of our ethical canons."[1] Another certification body said that they had received just 10 applications over the past decade from those with a cybercrime charge or conviction.

So, instead of attackers being generously rewarded for their exploits with a well-paying job in cybersecurity, the reality is just the opposite: they are severely restricted from virtually any job that uses technology.

Did you hear that one of the leading online password managers reported that attackers had stolen backups of customer password data as well as personal information (billing address, email addresses, telephone numbers, and IP addresses), and this was after the company had denied for over four months that any customer data was stolen? And that government researchers had discovered that suspected Russian attackers had infected and were lurking inside a U.S. satellite network? That a settlement based on a five-year-old data breach affecting hundreds of millions of U.S. citizens—with some states reporting almost 60 percent of its population as victims—was finally reached but only provides credit monitoring and identity restoration services to all victims? That a data breach of 427 gigabytes (GB) of data occurred on third-party software used by restaurants and hotels around the world? And that information security companies have been laying off hundreds of cyber workers in recent months due to an unsure economy?

And all of this happened in just over *one day*?

You may not have heard of any of these incidents. While in the past, just one of these cyber events would have made newsworthy headlines that immediately went viral across the Internet, today they barely register a blip on the radar screen. It's not because they are unimportant; rather, it's simply because cybersecurity attacks have become so commonplace that we hardly notice them any longer. *Oh, there was another data breach today? So, what else is new?*

The sheer volume of attacks has reached astronomical proportions. The AV-TEST Institute receives instances of over 450,000 new malicious programs (malware) and potentially unwanted applications (PUAs) each day. The total number of instances of malware has grown from 182 million in 2013 to over 1.34 billion today.[2] Cybercrime has been called the "greatest transfer of economic wealth in history." It is estimated that it could reach *$10.5 trillion annually* by 2025.[3] And the dismal numbers go on and on.

The need to identify and defend against these continual attacks has created a domain that is now at the very core of the information technology (IT) industry. Known as **information security**, this domain is concerned with protecting the secrecy of information, ensuring that it has not been altered and that it can be reliably accessed. Elements of information security include mitigating threats and vulnerabilities, applying security architectures, and managing and overseeing security operations.

The workforce that manages information security in an enterprise is usually divided into two broad categories. Information security **managerial personnel** administer and manage plans, policies, and people, while information security **technical personnel** are concerned with designing, configuring, installing, and maintaining technical security equipment. Within these two broad categories are four generally recognized types of security positions:

- **Chief information security officer (CISO)**. This person reports directly to the CIO. (Large enterprises may have more layers of management between this person and the CIO.) This person is responsible for assessing, managing, and implementing security.
- **Security manager**. The security manager reports to the CISO and supervises technicians, administrators, and security staff. Typically, a security manager works on tasks identified by the CISO and resolves issues identified by technicians. This position requires an understanding of configuration and operation but not necessarily technical mastery.

- **Security administrator**. The security administrator has both technical knowledge and managerial skills. A security administrator manages daily operations of security technology and may analyze and design security solutions within a specific entity as well as identify users' needs.
- **Security technician**. This is generally an entry-level position for a person who has the necessary technical skills. Technicians provide technical support to configure security hardware, implement security software, and diagnose and troubleshoot problems.

There is a desperate demand for these qualified security personnel. Despite the fact that the worldwide information security workforce has reached an all-time high of 4.7 million professionals and just under half a million new workers are added annually, there is still a global shortage of *3.4 million* workers in this field. The United States alone has more than 700,000 unfilled security jobs.[4]

When hiring workers for cybersecurity positions, an overwhelming majority of enterprises use the Computing Technology Industry Association (CompTIA) Security+ certification to verify security competency. Of the hundreds of security certifications currently available, Security+ is one of the most widely acclaimed security certifications. Because it is internationally recognized as validating a foundation level of security skills and knowledge, the Security+ certification has become the security baseline for today's IT security professionals.

Note 1

The value of a security certification for an IT professional is significant. Along with years of experience, sector employed, and geographic location, holding a security certification is considered one of the primary drivers to merit a higher salary. And over 60 percent of information technology workers continue to seek additional security certifications for growing their skills and staying current with security trends.[5]

The CompTIA Security+ certification is a vendor-neutral credential that requires passing the current certification exam SY0-701. A successful candidate has the knowledge and skills required to identify attacks, threats, and vulnerabilities; design a strong security architecture; implement security controls; be knowledgeable of security operations and incident response; and be well versed in governance, risk, and compliance requirements.

Note 2

The CompTIA Security+ certification meets the ISO 17024 standard and is approved by the U.S. Department of Defense (DoD) to fulfill multiple levels of the DoD 8140/8570.01-M directive. This directive outlines which cybersecurity certifications are approved to validate the skills for certain job roles.

This module introduces the foundations of information security that form the basis of the Security+ certification. It begins by defining information security and looks at attackers and their motivations. The module also investigates how attacks occur and the impacts of those attacks. It concludes by examining various resources of information security.

What Is Information Security?

Certification

1.1 Compare and contrast various types of security controls.

1.2 Summarize fundamental security concepts.

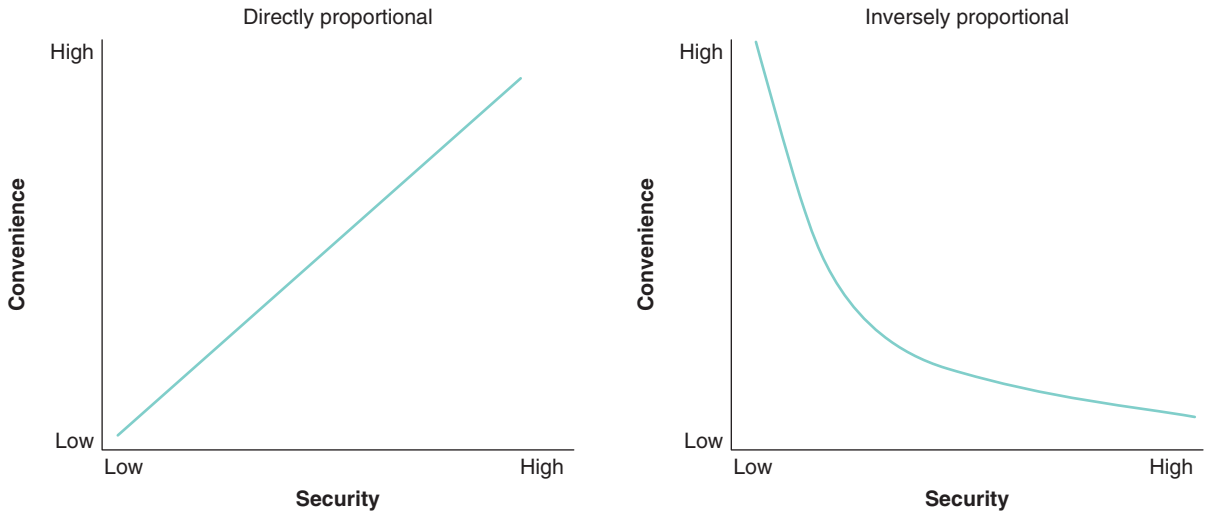
The first step in a study of information security is to define exactly what it is. This involves understanding security and knowing its basic principles. It also includes comparing information security to cybersecurity.

Understanding Security

The word *security* comes from the Latin, meaning "free from care." Sometimes security is defined as "the state of being free from danger," which is the **goal** of security. It is also defined as the "measures taken to ensure safety," which is the **process** of security. Since complete security can never be fully achieved, the focus of security is more often on the process instead of the goal. In this light, security can be defined as "the necessary steps to protect from harm."

It is important to understand the relationship between **security** and **convenience**. The relationship between these two is not **directly proportional** (*as security is increased, convenience is increased*) but, instead, it is completely the opposite, known as **inversely proportional** (*as security is increased, convenience is decreased*). As illustrated in Figure 1-1, inversely proportional means that when security increases (from *low* to *high* on the horizontal *x*-axis), convenience decreases (from *high* to *low* on the vertical *y*-axis).

Figure 1-1 Relationship of security to convenience



Note 3

In addition, as convenience is increased, usually security is decreased.

Consider a user who changes the screen timeout setting on their Apple iPhone from *Never* to *30 seconds* to minimize the risk of a thief stealing and using their phone. Although the security is increased, the convenience is decreased because they must now log in after 30 seconds of inactivity. Thus, the *more* secure something is, the *less* convenient it may be to use. Security is often described as sacrificing convenience for safety.

Principles of Security

There are several basic principles of security. These include security concepts and security controls.

Security Concepts

There are two fundamental security concepts. These are confidentiality, integrity, and availability and authentication, authorization, and accounting.

Confidentiality, Integrity, and Availability (CIA) Today security is usually focused on protecting information that provides value to people and enterprises. Three basic security protections must be extended over the information: **confidentiality, integrity, and availability (CIA)**. These may be defined as follows:

- **Confidentiality**. It is important that only approved individuals can access sensitive information. For example, the credit card number used to make an online purchase must be kept secure and

not made available to other parties. **Confidentiality** ensures that only authorized parties can view the information. Providing confidentiality can involve several different security tools, ranging from software to encrypt the credit card number stored on the web server to door locks to prevent access to those servers.

- **Integrity**. **Integrity** ensures that the information is correct and no unauthorized person or malicious software has altered the data. In the example of the online purchase, an attacker who could change the amount of a purchase from $10,000.00 to $1.00 would violate the integrity of the information.
- **Availability**. Information has value if the authorized parties who are assured of its integrity can access the information. **Availability** ensures that data is accessible to only authorized users and not to unapproved individuals. In this example, the total number of items ordered as the result of an online purchase must be available to an employee in a warehouse so that the correct items can be shipped to the customer but not made available to a competitor.

Authentication, Authorization, and Accounting (AAA) The second basic security principle, **authentication, authorization, and accounting (AAA;** sometimes called "triple-A"), involves controlling access to information. Consider this scenario. Suppose that Gabe is babysitting his sister Mia one afternoon. Before leaving the house, his mother tells Gabe that a package delivery service is coming to pick up a box, which is inside the front door. Soon there is a knock at the door, and as Gabe looks out, he sees the delivery person standing on the porch. Gabe asks them to display their employee credentials, which the delivery person is pleased to do, and then he opens the door to allow them inside—but only to the area by the front door to pick up the box. Gabe then signs the delivery person's tablet device so there is a confirmation record that the package was picked up.

This illustrates controlling access to information. The package delivery person first presents their ID to Gabe to be reviewed. A user accessing a computer system would likewise present credentials or **identification**, such as a username, when logging on to the system. Identification is the process of recognizing and distinguishing the user from any other user.

Checking the delivery person's credentials to be sure that they are authentic and not fabricated is **authentication**. Computer users, likewise, must have their credentials authenticated to ensure that they are who they claim to be. This is often done by entering a password, fingerprint scan, or other type of approved credentials.

Authorization, granting permission to take an action, is the next step. Gabe allowed the package delivery person to enter the house because their credentials were authentic. Likewise, once users have presented their identification and been authenticated, they can log in to a computer system. But what can they do once they have logged in? Gabe only allowed the package delivery person access to the area by the front door to retrieve the box; he did not allow them to go upstairs or into the kitchen. Likewise, computer users are granted access only to the specific services, devices, applications, and files needed to perform their job duties.

Gabe signing on the tablet is akin to **accounting**. Accounting creates a record that is preserved of who accessed the enterprise network, what resources they accessed, and when they disconnected from the network.

Note 4

Accounting data can be used not only to provide an audit trail but also for billing, determining trends, identifying resource usage, and future capacity planning.

AAA provides a framework for controlling access to computer resources. The basic steps in this access control process are summarized in Table 1-1.

Security Controls

A security **control** is a safeguard (sometimes called a **countermeasure**) that is employed within an enterprise to protect the CIA of information. A control attempts to limit the exposure of an asset to a danger. The four broad categories of controls are listed in Table 1-2.

Table 1-1 Basic steps in controlling access

Action	Description	Scenario example	Computer process
Identification	Review of credentials	Delivery person shows employee badge	User enters username
Authentication	Validate credentials as genuine	Gabe reads badge to determine it is real	User provides password
Authorization	Permission granted for admittance	Gabe opens door to allow delivery person in	User allowed to access only specific data
Accounting	Record of user actions	Gabe signs to confirm he picked up the package	Information recorded in log file

Table 1-2 Categories of controls

Control category	Description	Example
Managerial	Controls that use administrative methods	Acceptable use policy that specifies users should not visit malicious websites
Operational	Controls implemented and executed by people	Conducting workshops to help train users to identify and delete suspicious messages
Technical	Controls incorporated as part of hardware, software, or firmware	Hardware that blocks malicious content from entering the network
Physical	Controls that implement security in a defined structure and location	Installing a fence to prevent an unauthorized person from entering a building

Specific types of controls are found within these four broad categories:

- **Deterrent controls**. A **deterrent control** attempts to discourage security violations before they occur.
- **Preventive controls**. A **preventive control** works to prevent the threat from coming in contact with the vulnerability.
- **Detective controls**. A **detective control** identifies any threat that has reached the system.
- **Compensating controls**. A **compensating control** provides an alternative to normal controls that for some reason cannot be used.
- **Corrective controls**. A **corrective control** mitigates or lessens the damage caused by the incident.
- **Directive controls**. A **directive control** ensures that a particular outcome is achieved.

Note 5

One type of directive control is **incentive**, which is the "carrot" instead of the "stick." Incentives are often overlooked as a control, but they can be very powerful. One recent study looked at how incentive programs affected gym attendance. It found that gym goers who missed a workout but then received an extra incentive (in this case, bonus points that could be converted to cash) if they returned after a missed workout increased their gym visits by 27 percent compared with those who did not receive the incentive.[6]

These control types are summarized along with examples in Table 1-3.

Table 1-3 Control types

Control type	Description	When it occurs	Example
Deterrent control	Discourage attack	Before attack	Signs indicating that the area is under video surveillance
Preventive control	Prevent attack	Before attack	Security awareness training for all users
Directive control	Prevent attack	Before attack	An incentive to employees who pass a training course
Detective control	Identify attack	During attack	Installing motion detection sensors
Compensating control	Alternative to normal control	During attack	An infected computer is isolated on a different network
Corrective control	Lessen damage from attack	After attack	A virus is cleaned from an infected server

Caution !

Security professionals do not universally agree on the nomenclature and classification of control types. Some researchers divide control types into only managerial, operational, and technical, while others divide them into administrative, logical, and physical. Some security researchers specify up to18 different control types.

Cybersecurity versus Information Security

Different terms are sometimes used when describing security protections in an enterprise: **information security**, **computer security**, **IT security**, **cybersecurity**, and **information assurance**, to name just a few. Currently the two most used terms are *cybersecurity* and *information security*. Although they are often used as synonyms, strictly speaking, they are different.

Cybersecurity usually involves a range of practices, processes, and technologies intended to protect devices, networks, and programs that process and store data in an electronic form. Information security, on the other hand, protects "processed data" (information) that is essential in an enterprise business environment (more so than "raw data"). In addition, in a business, this information may be in any format, from electronic files to paper documents. Because business enterprises most often deal with information and that information is in a variety of formats, *information security* is often considered the most appropriate term used in this setting.

Note 6

Although there is no universal agreement on these definitions, generally speaking, *cybersecurity* is considered an overall umbrella term under which information security is found.

Defining Information Security

Information security describes the tasks of securing enterprise information often found in a digital format, whether it be manipulated by a microprocessor (such as on a laptop or file server), preserved on a storage device (like a hard drive or USB flash drive), or transmitted over a network (such as a local area network or the Internet). Yet information security cannot completely prevent successful attacks or guarantee that a system is totally secure, just as the security measures used in a house can never guarantee complete safety from a burglar. The goal of information security is to ensure that protective measures are properly implemented to ward off attacks, prevent the total collapse of the system when a successful attack does occur, and recover as quickly as possible. Thus, information security is, first and foremost, **protection**.

Caution

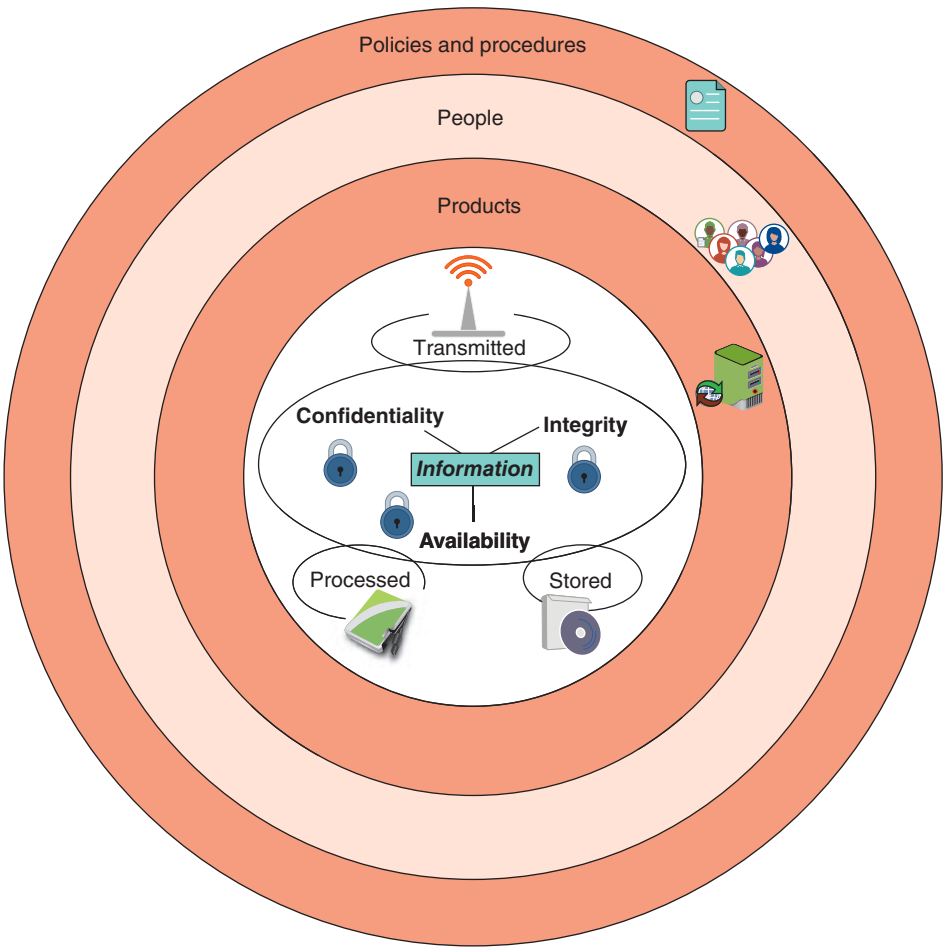
Information security should not be viewed as a war to be won or lost. Just as crimes such as burglary can never be completely eradicated, neither can cyberattacks. The goal is not a complete victory but instead maintaining equilibrium: as attackers take advantage of a weakness in a defense, defenders must respond with an improved defense. Information security is an endless cycle between attacker and defender.

Second, information security is intended to protect **information** that provides value to people and enterprises. CIA makes up the three basic protections that must be extended over information.

Because this information is often stored on computer hardware, manipulated by software, and transmitted by communications, each of these areas must be protected. The third objective of information security is to protect the CIA of information *on the devices that store, manipulate, and transmit the information*.

This protection is achieved through a process that is a combination of three entities. As shown in Figure 1-2, information and hardware, software, and communications are protected in three layers: **products**, **people**, and **policies and procedures**. The procedures enable people to understand how to use products to protect information.

Figure 1-2 Information security layers



Thus, information security may be defined as *that which protects the integrity, confidentiality, and availability of information through products, people, and procedures on the devices that store, manipulate, and transmit the information*.