

Eighth Edition

**Save 10%**  
on Exam Vouchers  
**Coupon Inside!**

CompTIA®  
**Security+**®  
**STUDY  
GUIDE**

**EXAM SY0-601**

Includes one year of **FREE** access after activation to the  
interactive online learning environment and study tools:

**2 custom practice exams**

**100 electronic flashcards**

**Searchable key term glossary**

**MIKE CHAPPLE  
DAVID SEIDL**

 **SYBEX**  
A Wiley Brand

# Table of Contents

[Cover](#)

[Title Page](#)

[Copyright](#)

[Dedication](#)

[Acknowledgments](#)

[About the Authors](#)

[About the Technical Editor](#)

[Introduction](#)

[The Security+ Exam](#)

[What Does This Book Cover?](#)

[Exam SY0-601 Exam Objectives](#)

[SY0-601 Certification Exam Objective Map](#)

[Assessment Test](#)

[Answers to Assessment Test](#)

[Chapter 1: Today's Security Professional](#)

[Cybersecurity Objectives](#)

[Data Breach Risks](#)

[Implementing Security Controls](#)

[Data Protection](#)

[Summary](#)

[Exam Essentials](#)

[Review Questions](#)

[Chapter 2: Cybersecurity Threat Landscape](#)

[Exploring Cybersecurity Threats](#)

[Threat Data and Intelligence](#)

[Summary](#)

[Exam Essentials](#)

[Review Questions](#)

## [Chapter 3: Malicious Code](#)

[Malware](#)

[Malicious Code](#)

[Adversarial Artificial Intelligence](#)

[Summary](#)

[Exam Essentials](#)

[Review Questions](#)

## [Chapter 4: Social Engineering, Physical, and Password Attacks](#)

[Social Engineering](#)

[Password Attacks](#)

[Physical Attacks](#)

[Summary](#)

[Exam Essentials](#)

[Review Questions](#)

## [Chapter 5: Security Assessment and Testing](#)

[Vulnerability Management](#)

[Security Vulnerabilities](#)

[Penetration Testing](#)

[Training and Exercises](#)

[Summary](#)

[Exam Essentials](#)

[Review Questions](#)

## [Chapter 6: Secure Coding](#)

[Software Assurance Best Practices](#)

[Designing and Coding for Security](#)  
[Software Security Testing](#)  
[Injection Vulnerabilities](#)  
[Exploiting Authentication Vulnerabilities](#)  
[Exploiting Authorization Vulnerabilities](#)  
[Exploiting Web Application Vulnerabilities](#)  
[Application Security Controls](#)  
[Secure Coding Practices](#)  
[Summary](#)  
[Exam Essentials](#)  
[Review Questions](#)

## [Chapter 7: Cryptography and the Public Key Infrastructure](#)

[An Overview of Cryptography](#)  
[Goals of Cryptography](#)  
[Cryptographic Concepts](#)  
[Modern Cryptography](#)  
[Symmetric Cryptography](#)  
[Asymmetric Cryptography](#)  
[Hash Functions](#)  
[Digital Signatures](#)  
[Public Key Infrastructure](#)  
[Asymmetric Key Management](#)  
[Cryptographic Attacks](#)  
[Emerging Issues in Cryptography](#)  
[Summary](#)  
[Exam Essentials](#)  
[Review Questions](#)

## [Chapter 8: Identity and Access Management](#)

[Identity](#)

[Authentication and Authorization](#)

[Authentication Methods](#)

[Accounts](#)

[Access Control Schemes](#)

[Summary](#)

[Exam Essentials](#)

[Review Questions](#)

## [Chapter 9: Resilience and Physical Security](#)

[Building Cybersecurity Resilience](#)

[Response and Recovery Controls](#)

[Physical Security Controls](#)

[Summary](#)

[Exam Essentials](#)

[Review Questions](#)

## [Chapter 10: Cloud and Virtualization Security](#)

[Exploring the Cloud](#)

[Virtualization](#)

[Cloud Infrastructure Components](#)

[Cloud Security Issues](#)

[Cloud Security Controls](#)

[Summary](#)

[Exam Essentials](#)

[Review Questions](#)

## [Chapter 11: Endpoint Security](#)

[Protecting Endpoints](#)

[Service Hardening](#)

[Operating System Hardening](#)

[Securing Embedded and Specialized Systems](#)

[Summary](#)

[Exam Essentials](#)

[Review Questions](#)

## [Chapter 12: Network Security](#)

[Designing Secure Networks](#)

[Secure Protocols](#)

[Attacking and Assessing Networks](#)

[Network Reconnaissance and Discovery Tools and Techniques](#)

[Summary](#)

[Exam Essentials](#)

[Review Questions](#)

## [Chapter 13: Wireless and Mobile Security](#)

[Building Secure Wireless Networks](#)

[Managing Secure Mobile Devices](#)

[Summary](#)

[Exam Essentials](#)

[Review Questions](#)

## [Chapter 14: Incident Response](#)

[Incident Response](#)

[Incident Response Data and Tools](#)

[Mitigation and Recovery](#)

[Summary](#)

[Exam Essentials](#)

[Review Questions](#)

## [Chapter 15: Digital Forensics](#)

[Digital Forensic Concepts](#)  
[Conducting Digital Forensics](#)  
[Reporting](#)  
[Digital Forensics and Intelligence](#)  
[Summary](#)  
[Exam Essentials](#)  
[Review Questions](#)

## [Chapter 16: Security Policies, Standards, and Compliance](#)

[Understanding Policy Documents](#)  
[Personnel Management](#)  
[Third-Party Risk Management](#)  
[Complying with Laws and Regulations](#)  
[Adopting Standard Frameworks](#)  
[Security Control Verification and Quality Control](#)  
[Summary](#)  
[Exam Essentials](#)  
[Review Questions](#)

## [Chapter 17: Risk Management and Privacy](#)

[Analyzing Risk](#)  
[Managing Risk](#)  
[Risk Analysis](#)  
[Disaster Recovery Planning](#)  
[Privacy](#)  
[Summary](#)  
[Exam Essentials](#)  
[Review Questions](#)

## [Answers to Review Questions](#)

[Chapter 1: Today's Security Professional](#)  
[Chapter 2: Cybersecurity Threat Landscape](#)  
[Chapter 3: Malicious Code](#)  
[Chapter 4: Social Engineering, Physical, and Password Attacks](#)  
[Chapter 5: Security Assessment and Testing](#)  
[Chapter 6: Secure Coding](#)  
[Chapter 7: Cryptography and the Public Key Infrastructure](#)  
[Chapter 8: Identity and Access Management](#)  
[Chapter 9: Resilience and Physical Security](#)  
[Chapter 10: Cloud and Virtualization Security](#)  
[Chapter 11: Endpoint Security](#)  
[Chapter 12: Network Security](#)  
[Chapter 13: Wireless and Mobile Security](#)  
[Chapter 14: Incident Response](#)  
[Chapter 15: Digital Forensics](#)  
[Chapter 16: Security Policies, Standards, and Compliance](#)  
[Chapter 17: Risk Management and Privacy](#)  
[Index](#)  
[End User License Agreement](#)

## List of Tables

### Chapter 5

[TABLE 5.1 CVSS attack vector metric](#)

[TABLE 5.2 CVSS attack complexity metric](#)

[TABLE 5.3 CVSS privileges required metric](#)



[TABLE 5.4 CVSS user interaction metric](#)

[TABLE 5.5 CVSS confidentiality metric](#)

[TABLE 5.6 CVSS integrity metric](#)

[TABLE 5.7 CVSS availability metric](#)

[TABLE 5.8 CVSS scope metric](#)

[TABLE 5.9 CVSS Qualitative Severity Rating Scale](#)

## Chapter 6

[TABLE 6.1 Code review method comparison](#)

## Chapter 7

[TABLE 7.1 Comparison of symmetric and asymmetric cryptography systems](#)

[TABLE 7.2 Digital certificate formats](#)

## Chapter 9

[TABLE 9.1 RAID levels, advantages, and disadvantages](#)

[TABLE 9.2 Secure data destruction options](#)

## Chapter 11

[TABLE 11.1 Common ports and services](#)

## Chapter 12

[TABLE 12.1 Example network ACLs](#)

[TABLE 12.2 Secure and unsecure protocols](#)

## Chapter 13

[TABLE 13.1 Wi-Fi standards, maximum theoretical speed, and frequencies](#)

[TABLE 13.2 Mobile device deployment and management options](#)

## Chapter 16

[TABLE 16.1 NIST Cybersecurity Framework implementation tiers](#)

# List of Illustrations

## Chapter 1

[FIGURE 1.1 The three key objectives of cybersecurity programs are confidentiality...](#)

[FIGURE 1.2 The three key threats to cybersecurity programs are disclosure, availability...](#)

## Chapter 2

[FIGURE 2.1 Logo of the hacktivist group Anonymous](#)

[FIGURE 2.2 Dark web market](#)

[FIGURE 2.3 Recent alert listing from the CISA website](#)

[FIGURE 2.4 FireEye Cybersecurity Threat Map](#)

## Chapter 3

[FIGURE 3.1 Client-server botnet control model](#)

[FIGURE 3.2 Peer-to-peer botnet control model](#)

[FIGURE 3.3 Fileless virus attack chain](#)

## Chapter 4

[FIGURE 4.1 John the Ripper](#)

## Chapter 5

[FIGURE 5.1 Qualys asset map](#)

[FIGURE 5.2 Configuring a Nessus scan](#)

[FIGURE 5.3 Sample Nessus scan report](#)

[FIGURE 5.4 Nessus scan templates](#)

[FIGURE 5.5 Disabling unused plug-ins](#)

[FIGURE 5.6 Configuring credentialed scanning](#)

[FIGURE 5.7 Choosing a scan appliance](#)

[FIGURE 5.8 Nessus vulnerability in the NIST National Vulnerability Database...](#)

[FIGURE 5.9 Nessus Automatic Updates](#)

[FIGURE 5.10 Nikto web application scanner](#)

[FIGURE 5.11 Arachni web application scanner](#)

[FIGURE 5.12 Nessus vulnerability scan report](#)

[FIGURE 5.13 Missing patch vulnerability](#)

[FIGURE 5.14 Unsupported operating system vulnerability](#)

[FIGURE 5.15 Debug mode vulnerability](#)

[FIGURE 5.16 FTP cleartext authentication vulnerability](#)

[FIGURE 5.17 Insecure SSL cipher vulnerability](#)

## Chapter 6

[FIGURE 6.1 High-level SDLC view](#)

[FIGURE 6.2 The Waterfall SDLC model](#)

[FIGURE 6.3 The Spiral SDLC model](#)

[FIGURE 6.4 Agile sprints](#)

[FIGURE 6.5 The CI/CD pipeline](#)

[FIGURE 6.6 Fagan code review](#)

[FIGURE 6.7 Account number input page](#)

[FIGURE 6.8 Account information page](#)

[FIGURE 6.9 Account information page after blind SQL injection](#)

[FIGURE 6.10 Account creation page](#)

[FIGURE 6.11 Zyxel router default password](#)

[FIGURE 6.12 Session authentication with cookies](#)

[FIGURE 6.13 Session cookie from CNN.com](#)

[FIGURE 6.14 Session replay](#)

[FIGURE 6.15 Example web server directory structure](#)

[FIGURE 6.16 Message board post rendered in a browser](#)

[FIGURE 6.17 XSS attack rendered in a browser](#)

[FIGURE 6.18 Web application firewall](#)

[FIGURE 6.19 SQL error disclosure](#)

## Chapter 7

[FIGURE 7.1 Vigenère cipher table](#)

[FIGURE 7.2 A simple transposition cipher in action](#)

[FIGURE 7.3 Enigma machine from the National Security Agency's National Crypt...](#)

[FIGURE 7.4 OpenStego steganography tool](#)

[FIGURE 7.5 Image with embedded message](#)

[FIGURE 7.6 Challenge-response authentication protocol](#)

[FIGURE 7.7 Symmetric key cryptography](#)

[FIGURE 7.8 Asymmetric key cryptography](#)

## Chapter 8

[FIGURE 8.1 CHAP challenge and response sequence](#)

[FIGURE 8.2 802.1 authentication architecture with EAP, RADIUS, and LDAP](#)

[FIGURE 8.3 Kerberos authentication process](#)

[FIGURE 8.4 LDAP organizational hierarchy](#)

[FIGURE 8.5 A Titan key USB security key](#)

[FIGURE 8.6 Google authenticator showing TOTP code generation](#)

[FIGURE 8.7 An HOTP PayPal token](#)

[FIGURE 8.8 FAR vs. FRR, with CRR shown](#)

[FIGURE 8.9 Linux/Unix file permissions](#)

[FIGURE 8.10 Windows file permissions](#)

## Chapter 9

[FIGURE 9.1 A bollard](#)

[FIGURE 9.2 An access control vestibule](#)

[FIGURE 9.3 A simple screened subnet network design](#)

## Chapter 10

[FIGURE 10.1 \(a\) Vertical scaling vs. \(b\) Horizontal scaling](#)

[FIGURE 10.2 Thin clients, such as this Samsung Google Chromebook, are suffic...](#)

[FIGURE 10.3 AWS Lambda function-as-a-service environment](#)

[FIGURE 10.4 HathiTrust is an example of community cloud computing.](#)

[FIGURE 10.5 AWS Outposts offer hybrid cloud capability.](#)

[FIGURE 10.6 Shared responsibility model for cloud computing](#)

[FIGURE 10.7 Cloud Reference Architecture](#)

[FIGURE 10.8 Cloud Controls Matrix excerpt](#)

[FIGURE 10.9 Type I hypervisor](#)

[FIGURE 10.10 Type II hypervisor](#)

[FIGURE 10.11 Provisioning a virtualized server in AWS](#)

[FIGURE 10.12 Connecting to an AWS virtual server instance with SSH](#)

[FIGURE 10.13 Connecting to an AWS virtual server instance with RDP](#)

[FIGURE 10.14 AWS Elastic Block Storage \(EBS\) volumes](#)

[FIGURE 10.15 AWS Simple Storage Service \(S3\) bucket](#)

[FIGURE 10.16 Enabling full-disk encryption on an EBS volume](#)

[FIGURE 10.17 Security\\_group restricting access to a cloud server](#)

[FIGURE 10.18 Creating a virtual private cloud](#)

[FIGURE 10.19 Creating an EC2 instance with CloudFormation JSON](#)

[FIGURE 10.20 Limiting the datacenter regions used for a Zoom meeting](#)

[FIGURE 11.1 UEFI secure boot high-level process](#)

[FIGURE 11.2 Host firewalls and IPS systems vs. network firewalls and IPS sys...](#)

[FIGURE 11.3 Services.msc showing Remote Desktop Services set to manual](#)

[FIGURE 11.4 Linux file permissions](#)

[FIGURE 11.5 A SCADA system showing PLCs and RTUs with sensors and equipment...](#)

## Chapter 12

[FIGURE 12.1 Inline IPS vs. passive IDS deployment using a tap or SPAN port](#)

[FIGURE 12.2 Communications before and after a man-in-the-middle attack](#)

[FIGURE 12.3 Reputation data for gmail.com](#)

[FIGURE 12.4 A SYN flood shown in Wireshark](#)

[FIGURE 12.5 A sample tracert for www.wiley.com](#)

[FIGURE 12.6 A sample pathping for www.wiley.com](#)

[FIGURE 12.7 A sample nmap scan from a system](#)

[FIGURE 12.8 theHarvester output for wiley.com](#)

[FIGURE 12.9 DNSEnum output for wiley.com](#)

[FIGURE 12.10 tcpdump of a segment of nmap port scanning](#)

[FIGURE 12.11 A Wireshark capture of a segment of nmap\\_ports scanning](#)

[FIGURE 12.12 A Cuckoo Sandbox analysis of a malware file](#)

## Chapter 13

[FIGURE 13.1 Point-to-point and point-to-multipoint network designs](#)

[FIGURE 13.2 Evil twin pretending to be a legitimate access point](#)

[FIGURE 13.3 A wireless heatmap showing the wireless signal available from an...](#)

[FIGURE 13.4 Overlap map of the North American 2.4 GHz Wi-Fi channels](#)

## Chapter 14

[FIGURE 14.1 The incident response cycle](#)

[FIGURE 14.2 Federal Continuity of Operations Planning stages](#)

[FIGURE 14.3 MITRE's ATT&CK framework example of attacks against cloud instan...](#)

[FIGURE 14.4 The Diamond Model of Intrusion Analysis](#)

[FIGURE 14.5 The Cyber Kill Chain](#)

[FIGURE 14.6 The AlienVault SIEM default dashboard](#)

[FIGURE 14.7 Trend analysis via a SIEM dashboard](#)

[FIGURE 14.8 Alerts and alarms in the AlienVault SIEM](#)

[FIGURE 14.9 Rule configuration in AlienVault](#)

[FIGURE 14.10 The Windows Event Viewer showing a security log with an audit e...](#)

## Chapter 15

[FIGURE 15.1 The order of volatility](#)

[FIGURE 15.2 A sample chain of custody form](#)



[FIGURE 15.3 Output from a completed FTK Imager image](#)

[FIGURE 15.4 FTK Imager's Memory Capture dialog box](#)

[FIGURE 15.5 FTK Imager's evidence item documentation](#)

[FIGURE 15.6 Selecting the type of image or data to import](#)

[FIGURE 15.7 Ingestion modules in Autopsy](#)

[FIGURE 15.8 Using the Autopsy file discovery tool to identify images in an i...](#)

[FIGURE 15.9 Timelining in Autopsy to identify events related to the investig...](#)

## Chapter 16

[FIGURE 16.1 Excerpt from CMS roles and responsibilities chart](#)

[FIGURE 16.2 Excerpt from UC Berkeley Minimum Security Standards for Electron...](#)

[FIGURE 16.3 NIST Cybersecurity Framework Core Structure](#)

[FIGURE 16.4 Asset Management Cybersecurity Framework](#)

[FIGURE 16.5 NIST Risk Management Framework](#)

[FIGURE 16.6 Windows Server 2019 Security Benchmark Excerpt](#)

## Chapter 17

[FIGURE 17.1 Risk exists at the intersection of a threat and a corresponding ...](#)

FIGURE 17.2 Qualitative risk assessments use subjective rating scales to evaluate risk.

FIGURE 17.3 (a) STOP tag attached to a device. (b) Residue remaining on device.

FIGURE 17.4 Risk register excerpt

FIGURE 17.5 Risk matrix

FIGURE 17.6 Cover sheets used to identify classified U.S. government information.



**Take the Next Step  
in Your IT Career**

**Save  
10%  
on Exam Vouchers\***

**(up to a \$35 value)**

\*Some restrictions apply. See web page for details.

**CompTIA®**

**Get details at  
[www.wiley.com/go/sybextestprep](http://www.wiley.com/go/sybextestprep)**

To get the discount code, you'll need to register and log on the test bank. Then go to Resources.



# **CompTIA® Security+®**

## **Study Guide Exam SY0-601**

**Eighth Edition**



**Mike Chapple  
David Seidl**



Copyright © 2021 by John Wiley & Sons, Inc., Indianapolis, Indiana

Published simultaneously in Canada

ISBN: 978-1-119-73625-7

ISBN: 978-1-119-73627-1 (ebk.)

ISBN: 978-1-119-73626-4 (ebk.)

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at [www.wiley.com/go/permissions](http://www.wiley.com/go/permissions).

**Limit of Liability/Disclaimer of Warranty:** The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or Web site may provide or recommendations it may make. Further, readers should be aware that Internet Web sites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services or to obtain technical support, please contact our Customer Care Department within the U.S. at (877) 762-2974, outside the U.S. at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at [booksupport.wiley.com](http://booksupport.wiley.com). For more information about Wiley products, visit [www.wiley.com](http://www.wiley.com).

**Library of Congress Control Number: 2020950197**

TRADEMARKS: Wiley, the Wiley logo, and the Sybex logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. CompTIA and Security+ are registered trademarks of CompTIA Properties, LLC. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.



*To my mother, Grace. Thank you for encouraging my love of writing since I first learned to pick up a pencil.*

*—Mike*

*To my niece Selah, whose imagination and joy in discovery inspires me every time I hear a new Hop Cheep story, and to my sister Susan and brother-in-law Ben who encourage her to bravely explore the world around them.*

*—David*

# Acknowledgments

Books like this involve work from many people, and as authors, we truly appreciate the hard work and dedication that the team at Wiley shows. We would especially like to thank senior acquisitions editor Kenyon Brown. We have worked with Ken on multiple projects and consistently enjoy our work with him.

We owe a great debt of gratitude to Runzhi “Tom” Song, Mike’s research assistant at Notre Dame. Tom’s assistance with the instructional materials that accompany this book was invaluable.

We also greatly appreciated the editing and production team for the book, including Tom Dinse, our project editor, who brought years of experience and great talent to the project; Nadean Tanner, our technical editor, who provided insightful advice and gave wonderful feedback throughout the book; and Saravanan Dakshinamurthy, our production editor, who guided us through layouts, formatting, and final cleanup to produce a great book. We would also like to thank the many behind-the-scenes contributors, including the graphics, production, and technical teams who make the book and companion materials into a finished product.

Our agent, Carole Jelen of Waterside Productions, continues to provide us with wonderful opportunities, advice, and assistance throughout our writing careers.

Finally, we would like to thank our families and significant others who support us through the late evenings, busy weekends, and long hours that a book like this requires to write, edit, and get to press.

## About the Authors

**Mike Chapple, Ph.D., CISSP, Security+**, is author of the best-selling *CISSP (ISC)<sup>2</sup> Certified Information Systems Security Professional Official Study Guide* (Sybex, 2021) and the *CISSP (ISC)<sup>2</sup> Official Practice Tests* (Sybex, 2021). He is an information security professional with two decades of experience in higher education, the private sector, and government.

Mike currently serves as Teaching Professor in the IT, Analytics, and Operations department at the University of Notre Dame's Mendoza College of Business, where he teaches undergraduate and graduate courses on cybersecurity, data management, and business analytics.

Before returning to Notre Dame, Mike served as executive vice president and chief information officer of the Brand Institute, a Miami-based marketing consultancy. Mike also spent four years in the information security research group at the National Security Agency and served as an active duty intelligence officer in the U.S. Air Force.

Mike is technical editor for *Information Security Magazine* and has written more than 25 books. He earned both his B.S. and Ph.D. degrees from Notre Dame in computer science and engineering. Mike also holds an M.S. in computer science from the University of Idaho and an MBA from Auburn University. Mike holds the Cybersecurity Analyst+ (CySA+), Security+, Certified Information Security Manager (CISM), Certified Cloud Security Professional (CCSP), and Certified Information Systems Security Professional (CISSP) certifications.

Learn more about Mike and his other security certification materials at his website, [CertMike.com](http://CertMike.com).

**David Seidl** is Vice President for Information Technology and CIO at Miami University. During his IT career, he has served in a variety of technical and information security roles including serving as the Senior Director for Campus Technology Services at the University of Notre Dame where he co-led Notre Dame's move to the cloud, and oversaw cloud operations, ERP, databases, identity management, and a broad range of other technologies and service. He also served as Notre Dame's Director of Information Security and led Notre Dame's information security program. He has taught information security and networking undergraduate courses as an instructor for Notre Dame's Mendoza College of Business, and has written books on security certification and cyberwarfare, including co-authoring *CISSP (ISC)<sup>2</sup> Official Practice Tests* (Sybex, 2021) as well as the previous editions of both this book and the companion *CompTIA CySA+ Practice Tests: Exam CS0-001*.

David holds a bachelor's degree in communication technology and a master's degree in information security from Eastern Michigan University, as well as CISSP, CySA+, Pentest+, GPEN, and GCIH certifications.

## About the Technical Editor



**Nadean H. Tanner**, Security+, CASP+, A+, Network+, CISSP, and many other industry certifications, is the manager of Consulting-Education Services for Mandiant/FireEye. Prior to Mandiant, she was the lead instructor at Rapid7, teaching vulnerability management, incident detection and response, and Metasploit. For more than 20 years, she has worked in academia as an IT director of a private school and technology instructor at the university level as well as working for the U.S. Department of Defense. Nadean is the author of the *Cybersecurity Blue Team Toolkit* (Wiley, 2019) and the *CompTIA CASP+ Practice Tests: Exam CAS-003* (Sybex, 2020).

# Introduction

If you're preparing to take the Security+ exam, you'll undoubtedly want to find as much information as you can about computer and physical security. The more information you have at your disposal and the more hands-on experience you gain, the better off you'll be when attempting the exam. This study guide was written with that in mind. The goal was to provide enough information to prepare you for the test, but not so much that you'll be overloaded with information that's outside the scope of the exam.

This book presents the material at an intermediate technical level. Experience with and knowledge of security concepts, operating systems, and application systems will help you get a full understanding of the challenges you'll face as a security professional.

We've included review questions at the end of each chapter to give you a taste of what it's like to take the exam. If you're already working in the security field, we recommend that you check out these questions first to gauge your level of expertise. You can then use the book mainly to fill in the gaps in your current knowledge. This study guide will help you round out your knowledge base before tackling the exam.

If you can answer 90 percent or more of the review questions correctly for a given chapter, you can feel safe moving on to the next chapter. If you're unable to answer that many correctly, reread the chapter and try the questions again. Your score should improve.