

Principles of Cybersecurity

SECOND EDITION

Linda K. Lavender

Cybersecurity and Network Administration Teacher
Virginia Beach City Public Schools,
Advanced Technology Center
Virginia Beach, Virginia

Correlates to objectives for Certiport IT Specialist—Cybersecurity, Certiport IT Specialist—Network Security, Cisco Certified Support Technician in Cybersecurity, and NOCTI Cybersecurity Fundamentals certifications

Publisher

The Goodheart-Willcox Company, Inc.

Tinley Park, IL

www.g-w.com

Copyright © 2025
by
The Goodheart-Willcox Company, Inc.

Previous edition copyright 2020

All rights reserved. No part of this work may be reproduced, stored, or transmitted in any form or by any electronic or mechanical means, including information storage and retrieval systems, except as permitted by U.S. copyright law, without the prior written permission of The Goodheart-Willcox Company, Inc.

ISBN 979-8-88817-183-7

1 2 3 4 5 6 7 8 9 – 25 – 28 27 26 25 24 23

The Goodheart-Willcox Company, Inc. Brand Disclaimer: Brand names, company names, and illustrations for products and services included in this text are provided for educational purposes only and do not represent or imply endorsement or recommendation by the author or the publisher.

The Goodheart-Willcox Company, Inc. Safety Notice: The reader is expressly advised to carefully read, understand, and apply all safety precautions and warnings described in this book or that might also be indicated in undertaking the activities and exercises described herein to minimize risk of personal injury or injury to others. Common sense and good judgment should also be exercised and applied to help avoid all potential hazards. The reader should always refer to the appropriate manufacturer's technical information, directions, and recommendations; then proceed with care to follow specific equipment operating instructions. The reader should understand these notices and cautions are not exhaustive.

The publisher makes no warranty or representation whatsoever, either expressed or implied, including but not limited to equipment, procedures, and applications described or referred to herein, their quality, performance, merchantability, or fitness for a particular purpose. The publisher assumes no responsibility for any changes, errors, or omissions in this book. The publisher specifically disclaims any liability whatsoever, including any direct, indirect, incidental, consequential, special, or exemplary damages resulting, in whole or in part, from the reader's use or reliance upon the information, instructions, procedures, warnings, cautions, applications, or other matter contained in this book. The publisher assumes no responsibility for the activities of the reader.

The Goodheart-Willcox Company, Inc. Internet Disclaimer: The Internet resources and listings in this Goodheart-Willcox Publisher product are provided solely as a convenience to you. These resources and listings were reviewed at the time of publication to provide you with accurate, safe, and appropriate information. Goodheart-Willcox Publisher has no control over the referenced websites and, due to the dynamic nature of the Internet, is not responsible or liable for the content, products, or performance of links to other websites or resources. Goodheart-Willcox Publisher makes no representation, either expressed or implied, regarding the content of these websites, and such references do not constitute an endorsement or recommendation of the information or content presented. It is your responsibility to take all protective measures to guard against inappropriate content, viruses, or other destructive elements.

Image Credits. Front cover: NicoElNino/Shutterstock.com

Case Study: vs148/Shutterstock.com

Ethical Issue: Ink Drop/Shutterstock.com

Visual elements on background: ioat/Shutterstock.com

Figure 12-8: Used under the Creative Commons Attribution ShareAlike 4.0 International (CC BY-SA 4.0) <https://creativecommons.org/licenses/by-sa/4.0/deed.en>; icons changed

Cybersecurity is the field of computer science related to protecting digital assets and computer systems against unauthorized or criminal access and use. The Bureau of Labor Statistics reports there are roughly 83,000 jobs in this area with a median salary of nearly \$90,000. It projects a growth of 37 percent through 2024. Demand for individuals with cybersecurity skills is expected to be very high. The Cybersecurity Council has reported an unprecedented demand for highly skilled cybersecurity practitioners. These individuals are needed for building security into new and existing networks. They also need to be capable of assessing security on a real-time basis. These individuals are the front-line defenders against cybersecurity threats across industries and governmental agencies.

Principles of Cybersecurity will prepare you with skills and knowledge needed in the field of cybersecurity. By studying this text, you will learn about security threats and vulnerabilities. In addition, you will learn how to identify these issues and how to combat them. This text also helps prepare you for certification in the following:

- Certiport Information Technology (IT) Specialist in Cybersecurity
- Certiport Information Technology (IT) Specialist in Network Security
- Cisco Certified Support Technician in Cybersecurity
- NOCTI Cybersecurity Fundamentals

Linda K. Lavender is a cybersecurity and network administration teacher for Virginia Beach City Public Schools, Advanced Technology Center. She is also an adjunct instructor in information technology for Tidewater Community College in Virginia Beach. She holds a Master of Science in Cybersecurity and a Bachelor of Science in Computer Information Systems from Saint Leo University, Florida. She has been named teacher of the year by several organizations, including ACTE. She is certified in CompTIA Security+, Network+, A+, CySA+, and CTT+, as well as certified as a Certiport Information Technology Specialist.

REVIEWERS

The author and publisher wish to thank the following industry and teaching professionals for their valuable input into the development of *Principles of Cybersecurity*.

Charles W. Brown Jr.

CATE Instructor
Central High School
Pageland, SC

Lisa-Marie Burns

Business Education Department
Chair
Washington High School Fremont
Unified School District
Fremont, CA

Kristin A. Burr

Business Teacher
Merritt Island High School
Merritt Island, FL

Norma Johnson Cancel

Business Marketing and Career
Education Instructor
Daleville High School
Daleville, AL

Jason T. Clark

Computer Systems Technology
Instructor
Appomattox County High School
Appomattox, VA

Florence Lynn Copeland

CTE Instructor
Chula Vista High School
San Diego, CA

Jason Cordes

Career and Technology Education
Teacher
Bryan Independent School District
Bryan, TX

Susan Crane

Business Education Teacher
Southern Alamance High School
Graham, NC

Paula F. Dana

Business Education Instructor
Darlington High School
Darlington, SC

Phyllis Bullock Eppes

Business Education Teacher
Powhatan High School
Powhatan, VA

Sharon Flanagan

Business Education Teacher
Sipsey Valley High School
Buhl, AL

Michael P. Harlen

Educator
Brookland-Cayce High School
Columbia, SC

Madison Holloman

Business Education Teacher
Irmo High School
Columbia, SC

Sharon Lambert

Business/Technology Teacher
Dunnellon High School (Marion
County Public Schools)
Dunnellon, FL

Donavon Lockett

Cyber Security Instructor
Advanced Technologies Academy
Las Vegas, NV

Shannon Lynch

Career & Technical Education
Teacher, Computer Technology
Southern Alamance High School
Graham, NC

Teri H. Mitchell

Career Tech Instructor–STEM,
Cyber, Computer Science
Challenger Middle School
Huntsville, AL

Renee Monteith

Business Teacher
Clover High School
Clover, SC

Stephen Morisani, Jr.

Mathematics and Computer
Science Instructor
Fairhope High School
Fairhope, AL

Darius Powell

Business Education Teacher
Sycamore High School
Cincinnati, OH

Sharon Ray, Ed.S.

Business Education and
Technology Teacher
Holly Pond High School
Holly Pond, AL

Javier Rios

Career and Technical Education
Instructor
JHF Polytechnic High School
Sun Valley, CA

Tracy C. Smith

Business Teacher–Career and
Technical Education
Fuquay-Varina High School
Fuquay-Varina, NC

Jessica Tibbs

Business and Information
Technology Teacher
Prince Edward County Public
Schools
Farmville, VA

Kathy Van Vleet

Technology Instructor
West Port High School
Ocala, FL

Melanie Weser

Teacher/Network Administrator
Peninsula Catholic High School
Newport News, VA

Mr. John Williams

CATE Computer Science and IT
Instructor
Whale Branch Early College High
School
Seabrook, SC

The second edition of *Principles of Cybersecurity* has been revised to reflect new and emerging topics in the cybersecurity field. In addition, the chapter content and visuals have been updated to reflect the ever-changing technological tools used in cybersecurity. An overview of the changes made to this edition has been provided.

- Content is tailored to cover topics discussed in four cybersecurity certifications:
 - Certiport Information Technology (IT) Specialist in Cybersecurity
 - Certiport Information Technology (IT) Specialist in Network Security
 - Cisco Certified Support Technician in Cybersecurity
 - NOCTI Cybersecurity Fundamentals
- Assessment activities and questions have been revised to fully correlate to measurable learning outcomes.
- Quick Look activities revised to be adapted to either Windows 10 or 11.
- Use of new and emerging terminology in the cybersecurity field such as *ethical* and *malicious hackers* as well as *closed* and *clear box testing*.
- Remodel of an entire chapter to focus specifically on common malware, vulnerabilities, and threats.
- New content focuses on new and emerging technologies such as artificial intelligence and personal cloud computing.
- New content introduces students to basic concepts of adding users in Linux programs in addition to Windows programs.
- Revision of content covering software vulnerabilities as well as the addition of protection methods.
- Compliance and frameworks content has been revised to reflect the latest laws as well as support materials affecting the cybersecurity field.
- New content discusses the history of computer forensics and common forensics frameworks.
- Coverage of career readiness topics expanded to include topics on researching careers and education options as well as writing cover messages as part of the application process.
- For digital users, a new Command Line Interface Management Handbook is a new module lesson provided on the Digital Companion.

Goodheart-Willcox appreciates the value of industry credentials, certifications, and accreditation. We are pleased to partner with leading organizations to support students and programs in achieving credentials. Integrating industry-recognized credentialing into a career and technical education (CTE) program provides many benefits for the student and for the institution. By achieving third-party certificates, students gain confidence, have proof of a measurable level of knowledge and skills, and earn a valuable achievement to include in their résumés. For educators and administrators, industry-recognized credentials and accreditation validate learning, enhance the credibility of programs, and provide valuable data to measure student performance and help guide continuous program improvement.

Principles of Cybersecurity is correlated to the Cybersecurity Fundamentals credential offered by NOCTI.

NOCTI NOCTI Certifications

Goodheart-Willcox is pleased to partner with NOCTI, a leading provider of industry certification solutions for CTE programs across the nation. With over 50 years of experience, NOCTI is a valuable partner in the CTE community's efforts to improve America's workforce. Goodheart-Willcox has created correlations between select products and the standards and competencies that make up the NOCTI credentials, to the benefit of states, instructors, and students working to achieve NOCTI credentials.

NOCTI certifications (knowledge-based and skill-based) are developed by national teams of subject matter experts as part of the process that meets personnel accrediting standards and requirements under ISO 17.024, resulting in credentials measuring skills and competencies critical for learner success outside the classroom. From online test delivery and psychometric services to digital badging and professional development, NOCTI uses the latest tools and methods to provide relevant solutions for those in CTE. For more information about NOCTI, visit www.nocti.org.

To see how *Principles of Cybersecurity* correlates to credentialing and certification standards, visit the Correlations tab at www.g-w.com/principles-of-cybersecurity-2025.

Student Tools

Student Text

Principles of Cybersecurity is an exciting, full-color, and highly illustrated learning resource that prepares students with skills needed in the cybersecurity field. This text will also help prepare students for industry-recognized certification. Students will learn a variety of cybersecurity topics as well as important employability skills for their future careers.



Lab Manual

- Hands-on practice includes questions and activities.
- Organized to follow the textbook chapters to help students achieve key learning outcomes.

G-W Digital Companion

- E-flash cards and vocabulary exercises allow interaction with content to create opportunities to increase achievement.
- Command Line Interface Management Handbook provides basic concepts as well as hands-on activities using PowerShell and the Linux shell.

Online Learning Suite

- Provides easy-to-use access and navigation.
- Includes accessible resources for all learners.
- Encourages practice and repetition.

Instructor Tools

LMS Integration

Integrate Goodheart-Willcox content within your Learning Management System for a seamless user experience for both you and your students. EduHub LMS-ready content in Common Cartridge® format facilitates single sign-on integration and gives you control of student enrollment and data. With a Common Cartridge integration, you can access the LMS features and tools you are accustomed to using and G-W course resources in one convenient location—your LMS.

G-W Common Cartridge provides a complete learning package for you and your students. The included digital resources help your students remain engaged and learn effectively:

- **Digital Textbook**
- Online **Lab Manual content**
- **Drill and Practice** vocabulary activities
- **Command Line Interface Management Handbook** module lesson

When you incorporate G-W content into your courses via Common Cartridge, you have the flexibility to customize and structure the content to meet the educational needs of your students. You may also choose to add your own content to the course.

For instructors, the Common Cartridge includes the Online Instructor Resources. QTI® question banks are available within the Online Instructor Resources for import into your LMS. These prebuilt assessments help you measure student knowledge and track results in your LMS gradebook. Questions and tests can be customized to meet your assessment needs.

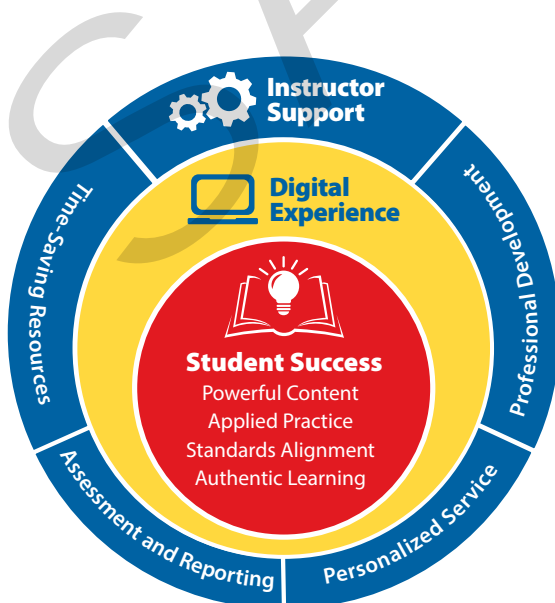
Online Instructor Resources

- The **Instructor Resources** provide instructors with time-saving preparation tools such as answer keys, editable lesson plans, and other teaching aids.
- **Instructor's Presentations for PowerPoint®** are fully customizable, richly illustrated slides that help you teach and visually reinforce the key concepts from each chapter.
- Administer and manage assessments to meet your classroom needs using **Assessment Software with Question Banks**, which include hundreds of multiple choice, completion, matching, and short answer questions to assess student knowledge of the content in each chapter.

See www.g-w.com/principles-of-cybersecurity-2025 for a list of all available resources.

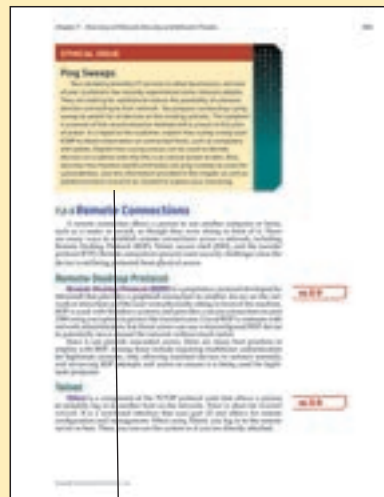
Professional Development

- Expert content specialists
- Research-based pedagogy and instructional practices
- Options for virtual and in-person Professional Development



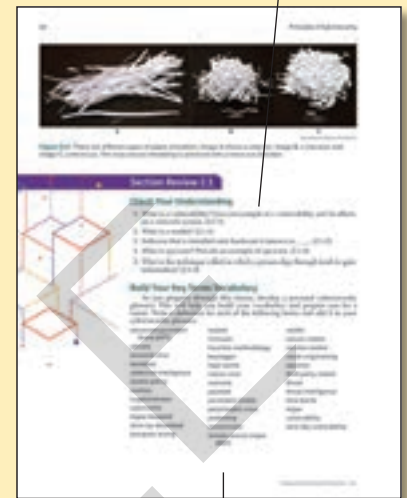


Case Study features present you with a scenario and ask you what action should be taken to connect your learning to real-life situations.



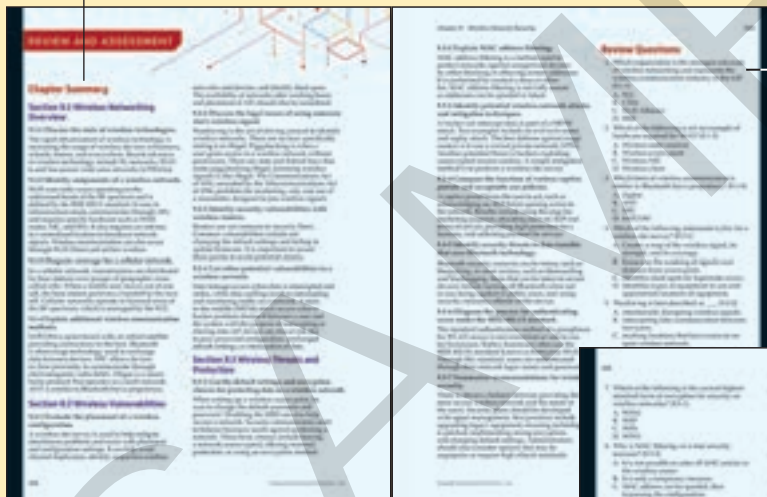
Ethical Issue features illustrate situations in which an ethical or moral judgment is needed.

Check Your Understanding questions at the end of each chapter section provide an opportunity to review what you have learned before moving on to additional content. Each question is tied to a Learning Outcome.



Build Your Key Terms Vocabulary activities review the key terms presented in each section. By completing these activities, you will be able to demonstrate your understanding of cybersecurity terms.

Chapter Summary presents key chapter concepts tied to each Learning Outcome for quick review.

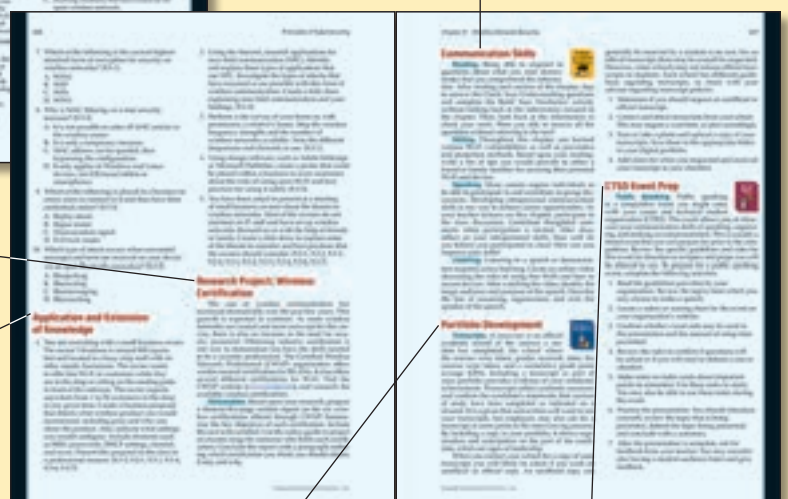


Review Questions cover the concepts presented in the chapter as well as are tied to the Learning Outcomes, which enables you to evaluate your understanding of the material.

Communication Skills activities provide ways for you to demonstrate the literacy and career-readiness skills you have mastered.

Research Project provides you with an opportunity to apply your research skills by investigating a topic in greater detail.

Application and Extension of Knowledge activities challenge you to relate what you learned in the chapter to your own ideas and projects. Each activity is tied to a Learning Outcome.



Portfolio Development activities provide guidance in creating a personal digital portfolio for use when exploring volunteer, education, training, and career opportunities.

CTSO Event Prep provides information to use when preparing for competitive activities in career and technical student organization (CTSO) competitions.

BRIEF CONTENTS

CHAPTER 1	Cybersecurity Basics.....	2
CHAPTER 2	Information Security Fundamentals.....	34
CHAPTER 3	Managing User Security.....	70
CHAPTER 4	Protecting and Controlling Physical Environments and Devices ...	118
CHAPTER 5	Protecting Host Systems.....	146
CHAPTER 6	Security Vulnerabilities and Protection of Nontraditional Hosts...	190
CHAPTER 7	Overview of Network Security and Network Threats.....	224
CHAPTER 8	Protecting Network Services and Infrastructure from Attacks...	262
CHAPTER 9	Wireless Network Security.....	294
CHAPTER 10	Encryption and Cryptography.....	328
CHAPTER 11	Software Vulnerabilities.....	368
CHAPTER 12	Evaluating System Compliance and Integrity.....	408
CHAPTER 13	Cloud Computing.....	442
CHAPTER 14	Risk Management.....	472
CHAPTER 15	Maintaining Operability.....	500
CHAPTER 16	Incident Response and Computer Forensics.....	530
CHAPTER 17	Career and Workplace Considerations.....	562

CHAPTER 1

Cybersecurity Basics.....2

- Section 1.1 Introduction to Cybersecurity..... 4
- Section 1.2 Skills Needed by Cybersecurity Professionals..... 17
- Section 1.3 Security Principles..... 24
- Review and Assessment 30

CHAPTER 2

Information Security Fundamentals.....34

- Section 2.1 Vulnerabilities and Threats..... 36
- Section 2.2 Users and Security Threats... 55
- Review and Assessment 66

CHAPTER 3

Managing User Security..... 70

- Section 3.1 Authentication and Control.. 72
- Section 3.2 Access to Files and Folders .. 95
- Section 3.3 User Management in Linux..106
- Review and Assessment 113

CHAPTER 4

Protecting and Controlling Physical Environments and Devices.....118

- Section 4.1 Business Controls 120
- Section 4.2 Environmental Controls... 128
- Section 4.3 Data Management Protection Controls 135
- Review and Assessment 142

CHAPTER 5

Protecting Host Systems..... 146

- Section 5.1 Operating System Services..... 148
- Section 5.2 System Vulnerabilities.... 172
- Review and Assessment 186

CHAPTER 6

Security Vulnerabilities and Protection of Nontraditional Hosts..... 190

- Section 6.1 Mobile Device Security ... 192
- Section 6.2 Nontraditional Hosts 211
- Review and Assessment 220

CHAPTER 7

Overview of Network Security and Network Threats 224

- Section 7.1 Network Basics..... 226
- Section 7.2 Network Threats 249
- Review and Assessment 259

CHAPTER 8

Protecting Network Services and Infrastructure from Attacks..... 262

- Section 8.1 Network Design 264
- Section 8.2 Protecting Network Devices 278
- Review and Assessment 290

CHAPTER 9

Wireless Network Security . . . 294

Section 9.1 Wireless Networking
Overview 296

Section 9.2 Wireless Vulnerabilities . . . 304

Section 9.3 Wireless Threats
and Protection 311

Review and Assessment 324

CHAPTER 10

Encryption and Cryptography . . 328

Section 10.1 Encryption Overview . . . 330

Section 10.2 Validating and Securing
Network Transmission 342

Section 10.3 Data Encryption
and Threats 354

Review and Assessment 364

CHAPTER 11

Software Vulnerabilities 368

Section 11.1 Managing Application
Software 370

Section 11.2 Threats to Web
Applications 383

Section 11.3 Threats to Databases . . . 395

Review and Assessment 403

CHAPTER 12

**Evaluating System Compliance
and Integrity 408**

Section 12.1 Frameworks
and Compliance 410

Section 12.2 Overview
of Penetration Testing 419

Review and Assessment 438

CHAPTER 13

Cloud Computing 442

Section 13.1 Cloud Basics 444

Section 13.2 Cloud Services 454

Section 13.3 Virtualized Machines . . . 462

Review and Assessment 468

CHAPTER 14

Risk Management 472

Section 14.1 Overview of Risk 474

Section 14.2 Responding to
and Reducing Risk 486

Review and Assessment 496

CHAPTER 15

Maintaining Operability 500

Section 15.1 Business Continuity
and Disaster Recovery 502

Section 15.2 Fault Tolerance
and Redundancy 512

Review and Assessment 526

CHAPTER 16

**Incident Response
and Computer Forensics 530**

Section 16.1 Incident Response 532

Section 16.2 Computer Forensics 542

Review and Assessment 558

CHAPTER 17

**Career and Workplace
Considerations 562**

Section 17.1 Workplace Readiness . . . 564

Section 17.2 Understanding Industries . . 580

Review and Assessment 591

Glossary 594

Index 612

CASE STUDY

Cybersecurity Podcasts	22
Cookies	46
Permissions	102
Server Room Environmental Controls	131
Performance Management	157
Critical Infrastructure	219
Subnet Masks	229
VLAN in Business	271
Wireless Laws and Regulations	307
Hashing Concerns	345
DBMSs	401
Penetration Test Executive Summary	434
SaaS-Based LMS	456
Responding to Risk	491
Continuity of Operations	511
NSA Insider Threat	555
Workplace Dress Code	566

ETHICAL ISSUE

WikiLeaks	14
Keyloggers	44
Biometric-Authentication Technology	79
AI and Physical Cybersecurity Measures	127
Governmental Obligations	162
Medical IoT Devices	207
Ping Sweeps	255
Workplace VPNs	277
Personal Hotspots	315
Encryption Privacy	340
Big Data	377
Computer Fraud and Abuse Act	415
Restriction of Cloud Services	450
Employee Responsibility in Risk Management	481
Data Backups	519
Confidential Information	536
Employment Eligibility	588

QUICK LOOK

CHAPTER 1

Cybersecurity Basics

1.1.1	Hacking Tools	7
1.1.2	Viewing Cyber Threat Maps	9
1.1.3	Report on Cyberwarfare	13
1.1.4	Bug-Bounty Program	15
1.2.1	Soft Skills Self-Assessment	19
1.2.2	Cybersecurity Ethics	20
1.3.1	Frameworks	28

CHAPTER 2

Information Security Fundamentals

2.1.1	Macro Programming	41
2.1.2	Antimalware Software	42
2.1.3	Threat Intelligence	43
2.1.4	Cookie Policy	45
2.1.5	Cookies with Google Chrome	47
2.1.6	Personal Data Online	51
2.1.7	Advanced Internet Search	52
2.2.1	Local DNS Cache	59
2.2.2	School AUP	61
2.2.3	Recognizing Phishing	62
2.2.4	California Online Privacy Protection Act	64

CHAPTER 3

Managing User Security

3.1.1	Passwords	74
3.1.2	Local Password Policies	77
3.1.3	Authentication Challenges	81
3.1.4	Mandatory Vacations	84
3.1.5	Local User Accounts	89
3.1.6	Secondary Logon	91
3.1.7	User Account Control Settings	93
3.2.1	Share Permissions	97
3.2.2	Shared Folders on a System	99
3.2.3	NTFS Permission Settings	101
3.2.4	Effective User Rights	103
3.3.1	Reviewing Linux Distributions	107

CHAPTER 4

Protecting and Controlling Physical Environments and Devices

4.1.1	Physical Access Control	125
4.2.1	Data Centers	130
4.2.2	Fire Safety	133
4.3.1	Asset and Inventory Systems	136
4.3.2	Identify Tools Used for System Recovery	138

CHAPTER 5

Protecting Host Systems

5.1.1	Manually Updating Windows Drivers	149
5.1.2	Viewing and Changing PowerShell Script Execution	151
5.1.3	Windows Host Services	153
5.1.4	Startup Programs and Scheduled Tasks	154
5.1.5	Parameters in Performance Monitor	158
5.1.6	Event Logs	163
5.1.7	Event Log Data	165
5.1.8	Event Log Backup	167
5.1.9	Audit Policy	169
5.2.1	Patch Management Software	173
5.2.2	Vulnerability Scanners	177
5.2.3	Windows Firewall	181

CHAPTER 6

Security Vulnerabilities and Protection of Nontraditional Hosts

6.1.1	BYOD Policies	194
6.1.2	Mobile Malware Threats	196
6.1.3	TPM Compatibility	199
6.1.4	QR Codes	201
6.1.5	Tracking Software	203
6.1.6	Metadata	204
6.1.7	IoT Security Risks	209
6.2.1	Point-of-Sale Data Breaches	214
6.2.2	Printer Security	215

CHAPTER 7

Overview of Network Security and Network Threats

7.1.1	Decimal and CIDR Address Formats	230
7.1.2	IPv4 Address Exploration	234
7.1.3	IPv6 Address Exploration	237
7.1.4	Wireshark Basics	242
7.1.5	UDP and TCP Information in Wireshark	244
7.1.6	Netstat Command	247
7.2.1	Ping and ICMP	252
7.2.2	Ping Sweep Software	254
7.2.3	Exploring the Telnet Interface	256

CHAPTER 8

Protecting Network Services and Infrastructure from Attacks

8.1.1	DNS Cache and Settings	267
8.1.2	DNS Response Resolution	269
8.1.3	VPN Client Setup	276
8.2.1	Local ARP Cache and Traffic	281
8.2.2	Local Routing Table	283

QUICK LOOK (continued)

CHAPTER 9

Wireless Network Security

9.1.1	CTIA	297
9.2.1	Wardriving Tools	306
9.2.2	Router Security Vulnerabilities	308
9.3.1	MAC Addresses	317
9.3.2	Free Wi-Fi	319

CHAPTER 10

Encryption and Cryptography

10.1.1	Vigenère Cipher	333
10.1.2	Steganography in Practice	339
10.2.1	Hash Output	344
10.2.2	Digital Signature in Microsoft Windows Driver Files	346
10.2.3	Certificate Authorities	348
10.2.4	Web Page Security	349
10.2.5	Viewing a Certificate	352
10.3.1	EFS File Encryption	357
10.3.2	Linux Passwords and Hashes	359

CHAPTER 11

Software Vulnerabilities

11.1.1	Group Policy Management	373
11.1.2	AppLocker	376
11.1.3	GitHub	378
11.1.4	Windows Defender	379
11.2.1	Clearing Browser Cache	385
11.2.2	Web-Application Scanner	387
11.2.3	Buffer-Overflow Attack	389
11.2.4	Easter Eggs	392
11.2.5	OWASP Website	393
11.3.1	SQL Use	398
11.3.2	SQL Injection	400

CHAPTER 12

Evaluating System Compliance and Integrity

12.1.1	NIST Cybersecurity Framework	412
12.2.1	Social Engineering Pretext	423
12.2.2	Intelligence Gathering	427
12.2.3	Nmap	430
12.2.4	Encoded Data	432
12.2.5	Penetration Test Report	435
12.2.6	US Code for Computer Crime	437

CHAPTER 13

Cloud Computing

13.1.1	Private Cloud	448
13.1.2	Cloud Vendor Terms of Service	449
13.2.1	Google SaaS Offerings	456
13.2.2	IaaS Vendors	459
13.2.3	SECaaS Solutions	461
13.3.1	Installing VirtualBox	465

CHAPTER 14

Risk Management

14.1.1	Assets at Risk	477
14.1.2	Risk Factors	479
14.1.3	SLE, ARO, and ALE	483
14.2.1	Risk Response	489
14.2.2	CVE Information	490
14.2.3	Security Policy Types	495

CHAPTER 15

Maintaining Operability

15.1.1	FEMA Ready Program	504
15.1.2	Disaster-Recovery Plans	510
15.2.1	Evaluating Site Choices	514
15.2.2	Windows Archive Settings	521
15.2.3	Windows Backup Program	523
15.2.4	Viewing UPS Systems	524

CHAPTER 16

Incident Response and Computer Forensics

16.1.1	Incident Scoring	537
16.1.2	CSIRT Team	541
16.2.1	Hex to Decimal	548
16.2.2	Hex to ASCII	549
16.2.3	Hex Editor	551
16.2.4	Exif Data	552
16.2.5	Alternate Data Stream	554
16.2.6	Computer Forensics Certification	557

CHAPTER 17

Career and Workplace Considerations

17.1.1	Diversity Awareness	567
17.1.2	CSV File Format	571
17.1.3	Occupational Outlook Handbook	572
17.1.4	OSHA	575
17.1.5	CTSOs	579
17.2.1	Mission Statement	581
17.2.2	Bullying	584
17.2.3	Form W-4	588