

Fundamentals of Information Systems Security

FOURTH EDITION

David Kim | Michael G. Solomon



JONES & BARTLETT
LEARNING



World Headquarters

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

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

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

Copyright © 2023 by Jones & Bartlett Learning, LLC, an Ascend Learning Company

All rights reserved. No part of the material protected by this copyright may be reproduced or utilized in any form, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the copyright owner.

The content, statements, views, and opinions herein are the sole expression of the respective authors and not that of Jones & Bartlett Learning, LLC. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not constitute or imply its endorsement or recommendation by Jones & Bartlett Learning, LLC and such reference shall not be used for advertising or product endorsement purposes. All trademarks displayed are the trademarks of the parties noted herein. *Fundamentals of Information Systems Security, Fourth Edition* is an independent publication and has not been authorized, sponsored, or otherwise approved by the owners of the trademarks or service marks referenced in this product.

There may be images in this book that feature models; these models do not necessarily endorse, represent, or participate in the activities represented in the images. Any screenshots in this product are for educational and instructive purposes only. Any individuals and scenarios featured in the case studies throughout this product may be real or fictitious but are used for instructional purposes only.

24458-8

Production Credits

Vice President, Product Management: Marisa R. Urbano
Vice President, Product Operations: Christine Emerton
Director, Content Management: Donna Gridley
Director, Project Management and Content Services:
Karen Scott
Product Manager: Ned Hinman
Content Strategist: Melissa Duffy
Content Coordinator: Mark Restuccia
Development Editor: Kim Lindros
Technical Editor: Jeffrey Parker
Project Manager: Jessica deMartin

Senior Project Specialist: Jennifer Risdén
Digital Project Specialist: Rachel DiMaggio
Marketing Manager: Suzy Balk
Product Fulfillment Manager: Wendy Kilborn
Composition: Straive
Cover Design: Briana Yates
Media Development Editor: Faith Brosnan
Rights Specialist: Benjamin Roy
Cover Image (Title Page, Front Matter Opener, Part
Opener, Chapter Opener): © Ornithopter/Shutterstock
Printing and Binding: McNaughton & Gunn

Library of Congress Cataloging-in-Publication Data

Names: Kim, David (Information technology security consultant) | Solomon, Michael (Michael G.), 1963– author.
Title: Fundamentals of information systems security / David Kim, Michael G. Solomon.
Description: Fourth edition. | Burlington, Massachusetts : Jones & Bartlett Learning, [2023] | Includes bibliographical references and index.
Identifiers: LCCN 2021021301 | ISBN 9781284220735 (paperback)
Subjects: LCSH: Computer security. | Computer networks—Security measures. | Information storage and retrieval systems—Security measures.
Classification: LCC QA76.9.A25 K536 2023 | DDC 005.8—dc23
LC record available at https://protect-us.mimecast.com/s/jX-ACeRYDytkr095Spo_zs?domain=lcen.loc.gov

6048

Printed in the United States of America

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

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

—David Kim

To God, who has richly blessed me in so many ways.

—Michael G. Solomon

Contents

Preface	xviii
Acknowledgments	xix
New to This Edition	xxi
The Authors	xxii

PART I

The Need for Information Security 1

CHAPTER 1

Information Systems Security 2

Information Systems Security 3

Risks, Threats, and Vulnerabilities 9

What Is Information Systems Security? 10

Compliance Laws and Regulations Drive the Need for Information Systems Security 10

Tenets of Information Systems Security 13

Confidentiality 14

Integrity 16

Availability 16

The Seven Domains of a Typical IT Infrastructure 18

User Domain 18

Workstation Domain 21

LAN Domain 23

LAN-to-WAN Domain 25

WAN Domain 28

Remote Access Domain 32

System/Application Domain 36

Weakest Link in the Security of an IT Infrastructure 39

Ethics and the Internet 39

IT Security Policy Framework 39

Definitions 40

Foundational IT Security Policies 41

Data Classification Standards 42

CHAPTER SUMMARY 43

KEY CONCEPTS AND TERMS 43

CHAPTER 1 ASSESSMENT 44

CHAPTER 2**Emerging Technologies Are Changing How We Live 46****Evolution of the Internet of Things 48****Converting to a TCP/IP World 50****IoT's Impact on Human and Business Life 50**

How People Like to Communicate 51

IoT Applications That Impact Our Lives 51

Evolution from Brick and Mortar to E-Commerce 55**Why Businesses Must Have an Internet and IoT Marketing Strategy 57****IP Mobility 57**

Mobile Users and Bring Your Own Device 58

Mobile Applications 59

IP Mobile Communications 60

New Challenges Created by the IoT 61

Security 61

Privacy 63

Interoperability and Standards 65

Legal and Regulatory Issues 67

E-Commerce and Economic Development Issues 68

CHAPTER SUMMARY 69**KEY CONCEPTS AND TERMS 70****CHAPTER 2 ASSESSMENT 70****CHAPTER 3****Risks, Threats, and Vulnerabilities 72****Risk Management and Information Security 73**

Risk Terminology 74

Elements of Risk 75

Purpose of Risk Management 76

The Risk Management Process 76

Identify Risks 78

Assess and Prioritize Risks 79

Plan a Risk Response Strategy 83

Implement the Risk Response Plan 86

Monitor and Control Risk Response 89

IT and Network Infrastructure 90

Intellectual Property 91

Finances and Financial Data 92

Service Availability and Productivity 92

Reputation 93

Who Are the Perpetrators? 93

Risks, Threats, and Vulnerabilities in an IT Infrastructure 94

Threat Targets 97

Threat Types 97

What Is a Malicious Attack? 100

Birthday Attacks 101

Brute-Force Password Attacks 101

Credential Harvesting and Stuffing 101

Dictionary Password Attacks 102

IP Address Spoofing 102

Hijacking 102

Replay Attacks 103

Man-in-the-Middle Attacks 103

Masquerading 104

Eavesdropping 104

Social Engineering 104

Phreaking 105

Phishing 105

Pharming 106

What Are Common Attack Vectors? 107

Social Engineering Attacks 107

Wireless Network Attacks 108

Web Application Attacks 109

The Importance of Countermeasures 110

CHAPTER SUMMARY 111

KEY CONCEPTS AND TERMS 112

CHAPTER 3 ASSESSMENT 112

CHAPTER 4

Business Drivers of Information Security 114

Risk Management’s Importance to the Organization 115

Understanding the Relationship between a BIA, a BCP, and a DRP 118

Business Impact Analysis (BIA) 118

Business Continuity Plan (BCP) 119

Disaster Recovery Plan (DRP) 121

Assessing Risks, Threats, and Vulnerabilities 125

Closing the Information Security Gap 126

Adhering to Compliance Laws 127

Keeping Private Data Confidential 131

Mobile Workers and Use of Personally Owned Devices 132

BYOD Concerns 133

Endpoint and Device Security 134

	CHAPTER SUMMARY	135
	KEY CONCEPTS AND TERMS	136
	CHAPTER 4 ASSESSMENT	136
PART II	Securing Today's Information Systems	139
CHAPTER 5	Networks and Telecommunications	140
	The Open Systems Interconnection Reference Model	141
	The Main Types of Networks	142
	Wide Area Networks	143
	Local Area Networks	146
	TCP/IP and How It Works	148
	TCP/IP Overview	148
	IP Addressing	149
	Common Ports	150
	Common Protocols	151
	Internet Control Message Protocol	152
	Network Security Risks	153
	Categories of Risk	153
	Basic Network Security Defense Tools	155
	Firewalls	155
	Virtual Private Networks and Remote Access	160
	Network Access Control	162
	Voice and Video in an IP Network	162
	Wireless Networks	163
	Wireless Access Points	164
	Wireless Network Security Controls	164
	CHAPTER SUMMARY	167
	KEY CONCEPTS AND TERMS	167
	CHAPTER 5 ASSESSMENT	168
CHAPTER 6	Access Controls	169
	Four-Part Access Control	170
	Two Types of Access Controls	170
	Physical Access Control	171
	Logical Access Control	171
	Authorization Policies	173
	Methods and Guidelines for Identification	173
	Identification Methods	174
	Identification Guidelines	174

Processes and Requirements for Authentication	174
Authentication Types	175
Single Sign-On	185
Policies and Procedures for Accountability	187
Log Files	187
Monitoring and Reviewing	188
Data Retention, Media Disposal, and Compliance Requirements	188
Formal Models of Access Control	190
Discretionary Access Control	190
Operating Systems–Based DAC	191
Mandatory Access Control	193
Nondiscretionary Access Control	193
Rule-Based Access Control	193
Access Control Lists	194
Role-Based Access Control	195
Content-Dependent Access Control	196
Constrained User Interface	197
Other Access Control Models	197
Effects of Breaches in Access Control	199
Threats to Access Controls	200
Effects of Access Control Violations	201
Credential and Permissions Management	202
Centralized and Decentralized Access Control	202
Types of AAA Servers	203
Decentralized Access Control	205
Privacy	206
CHAPTER SUMMARY	211
KEY CONCEPTS AND TERMS	211
CHAPTER 6 ASSESSMENT	212

CHAPTER 7

Cryptography	214
What Is Cryptography?	215
Basic Cryptographic Principles	216
A Brief History of Cryptography	217
Cryptography's Role in Information Security	219
Business and Security Requirements for Cryptography	222
Internal Security	222
Security in Business Relationships	223
Security Measures That Benefit Everyone	223
Cryptographic Principles, Concepts, and Terminology	224
Cryptographic Functions and Ciphers	224

Types of Ciphers	228
Transposition Ciphers	228
Substitution Ciphers	228
Product and Exponentiation Ciphers	230
Symmetric and Asymmetric Key Cryptography	231
Symmetric Key Ciphers	231
Asymmetric Key Ciphers	232
Cryptanalysis and Public Versus Private Keys	233
Keys, Keyspace, and Key Management	236
Cryptographic Keys and Keyspace	236
Key Management	237
Key Distribution	238
Key Distribution Centers	239
Digital Signatures and Hash Functions	239
Hash Functions	239
Digital Signatures	240
Cryptographic Applications and Uses in Information System Security	241
Other Cryptographic Tools and Resources	242
Symmetric Key Standards	242
Asymmetric Key Solutions	245
Hash Function and Integrity	247
Digital Signatures and Nonrepudiation	249
Principles of Certificates and Key Management	250
Modern Key Management Techniques	251
CHAPTER SUMMARY	253
KEY CONCEPTS AND TERMS	253
CHAPTER 7 ASSESSMENT	253
CHAPTER 8	Malicious Software and Attack Vectors
	255
Characteristics, Architecture, and Operations of Malicious Software	256
The Main Types of Malware	257
Viruses	257
Spam	265
Worms	266
Trojan Horses	267
Logic Bombs	268
Active Content Vulnerabilities	269
Malicious Add-Ons	269
Injection	269
Botnets	270
Denial of Service Attacks	270
Spyware	273
Adware	273
Phishing	273

Keystroke Loggers 274
 Hoaxes and Myths 274
 Homepage Hijacking 275
 Webpage Defacements 275

A Brief History of Malicious Code Threats 276

1970s and Early 1980s: Academic Research and UNIX 276
 1980s: Early PC Viruses 277
 1990s: Early LAN Viruses 277
 Mid-1990s: Smart Applications and the Internet 277
 2000 to the Present 278

Threats to Business Organizations 279

Types of Threats 279
 Internal Threats from Employees 280

Anatomy of an Attack 281

What Motivates Attackers? 281
 The Purpose of an Attack 281
 Types of Attacks 282
 Phases of an Attack 283

Attack Prevention Tools and Techniques 289

Application Defenses 289
 Operating System Defenses 290
 Network Infrastructure Defenses 291
 Safe Recovery Techniques and Practices 292
 Implementing Effective Software Best Practices 292

Intrusion Detection Tools and Techniques 292

Antivirus Scanning Software 293
 Network Monitors and Analyzers 293
 Content/Context Filtering and Logging Software 293
 Honey pots and Honey nets 294

CHAPTER SUMMARY 295

KEY CONCEPTS AND TERMS 295

CHAPTER 8 ASSESSMENT 295

CHAPTER 9

Security Operations and Administration 297

Security Administration 298

Controlling Access 299
 Documentation, Procedures, and Guidelines 299
 Disaster Assessment and Recovery 300
 Security Outsourcing 300

Compliance 302

Event Logs 302
 Compliance Liaison 302
 Remediation 303

Professional Ethics	303
Common Fallacies About Ethics	304
Codes of Ethics	304
Personnel Security Principles	305
The Infrastructure for an IT Security Policy	308
Policies	309
Standards	311
Procedures	311
Baselines	312
Guidelines	313
Data Classification Standards	313
Information Classification Objectives	314
Examples of Classification	314
Classification Procedures	314
Assurance	315
Configuration Management	316
Hardware Inventory and Configuration Chart	316
The Change Management Process	317
Change Control Management	317
Change Control Committees	318
Change Control Procedures	319
Change Control Issues	320
Application Software Security	320
The System Life Cycle	320
Testing Application Software	322
Software Development and Security	325
Software Development Models	326
CHAPTER SUMMARY	330
KEY CONCEPTS AND TERMS	330
CHAPTER 9 ASSESSMENT	331

CHAPTER 10

Auditing, Testing, and Monitoring	333
Security Auditing and Analysis	334
Security Controls Address Risk	335
Determining What Is Acceptable	335
Permission Levels	336
Areas of Security Audits	337
Purpose of Audits	337
Customer Confidence	338
Defining the Audit Plan	340
Defining the Scope of the Plan	340
Auditing Benchmarks	341

Audit Data Collection Methods 343
 Areas of Security Audits 343
 Control Checks and Identity Management 344

Post-Audit Activities 345
 Exit Interview 345
 Data Analysis 345
 Generation of Audit Report 345
 Presentation of Findings 346

Security Monitoring 346
 Security Monitoring for Computer Systems 347
 Monitoring Issues 348
 Logging Anomalies 349
 Log Management 349

Types of Log Information to Capture 350

How to Verify Security Controls 352
 Intrusion Detection System 352
 Analysis Methods 353
 HIDS 354
 Layered Defense: Network Access Control 355
 Control Checks: Intrusion Detection 355
 Host Isolation 355
 System Hardening 356

Monitoring and Testing Security Systems 359
 Monitoring 359
 Testing 359

CHAPTER SUMMARY 367
KEY CONCEPTS AND TERMS 367
CHAPTER 10 ASSESSMENT 368

CHAPTER 11

Contingency Planning 369

Business Continuity Management 370
 Emerging Threats 371
 Static Environments 372
 Terminology 373
 Assessing Maximum Tolerable Downtime 375
 Business Impact Analysis 375
 Plan Review 377
 Testing the Plan 377

Backing Up Data and Applications 379
 Types of Backups 379

Incident Handling 380
 Preparation 380

Identification	381
Notification	381
Response	382
Recovery	383
Follow-Up	383
Documentation and Reporting	383
Recovery from a Disaster	383
Activating the Disaster Recovery Plan	384
Operating in a Reduced/Modified Environment	384
Restoring Damaged Systems	385
Disaster Recovery Issues	385
Recovery Alternatives	386
Interim or Alternate Processing Strategies	386
CHAPTER SUMMARY	389
KEY CONCEPTS AND TERMS	389
CHAPTER 11 ASSESSMENT	390

CHAPTER 12

Digital Forensics	391
Introduction to Digital Forensics	392
Understanding Digital Forensics	393
Knowledge That Is Needed for Forensic Analysis	394
Overview of Computer Crime	395
Types of Computer Crime	396
The Impact of Computer Crime on Forensics	396
Forensic Methods and Labs	398
Forensic Methodologies	398
Setting Up a Forensic Lab	400
Collecting, Seizing, and Protecting Evidence	401
The Importance of Proper Evidence Handling	402
Imaging Original Evidence	403
Recovering Data	404
Undeleting Data	404
Recovering Data from Damaged Media	405
Operating System Forensics	406
Internals and Storage	407
Command-Line Interface and Scripting	407
Mobile Forensics	408
Mobile Device Evidence	409
Seizing Evidence from a Mobile Device	409
CHAPTER SUMMARY	411
KEY CONCEPTS AND TERMS	411
CHAPTER 12 ASSESSMENT	411

PART III **Information Security Standards, Certifications, and Laws** **413**

CHAPTER 13

Information Security Standards **414**

Standards Organizations **415**

National Institute of Standards and Technology	415
International Organization for Standardization	417
International Electrotechnical Commission	419
World Wide Web Consortium	419
Internet Engineering Task Force	420
Institute of Electrical and Electronics Engineers	422
International Telecommunication Union Telecommunication Sector	423
American National Standards Institute	424
European Telecommunications Standards Institute Cyber Security Technical Committee	425

ISO 17799 (Withdrawn) **425**

ISO/IEC 27002	426
Payment Card Industry Data Security Standard	427

CHAPTER SUMMARY **429**

KEY CONCEPTS AND TERMS **429**

CHAPTER 13 ASSESSMENT **430**

CHAPTER 14

Information Security Certifications **431**

U.S. Department of Defense/Military Directive 8570.01 **432**

U.S. DoD/Military Directive 8140	432
U.S. DoD Training Framework	434

Vendor-Neutral Professional Certification

International Information Systems Security Certification Consortium, Inc.	437
Global Information Assurance Certification/SANS Institute	440
Certified Internet Web Professional	440
CompTIA	444
ISACA®	444
Other Information Systems Security Certifications	444

Vendor-Specific Professional Certifications **446**

Cisco Systems	447
Juniper Networks	447
RSA	448
Symantec	449
Check Point	450

CHAPTER SUMMARY **451**

KEY CONCEPTS AND TERMS **452**

CHAPTER 14 ASSESSMENT **452**

CHAPTER 15

Compliance Laws	454
Compliance Is the Law	455
Federal Information Security	459
The Federal Information Security Management Act of 2002	459
The Federal Information Security Modernization Act of 2014	461
The Role of the National Institute of Standards and Technology	461
National Security Systems	463
The Health Insurance Portability and Accountability Act (HIPAA)	464
Purpose and Scope	464
Main Requirements of the HIPAA Privacy Rule	465
Main Requirements of the HIPAA Security Rule	466
Oversight	468
Omnibus Regulations	469
The Gramm-Leach-Bliley Act	470
Purpose and Scope	471
Main Requirements of the GLBA Privacy Rule	472
Main Requirements of the GLBA Safeguards Rule	473
Oversight	474
The Sarbanes-Oxley Act	474
Purpose and Scope	474
SOX Control Certification Requirements	475
SOX Records Retention Requirements	476
Oversight	477
The Family Educational Rights and Privacy Act	477
Purpose and Scope	478
Main Requirements	478
Oversight	479
The Children's Online Privacy Protection Act of 1998	480
The Children's Internet Protection Act	480
Purpose and Scope	480
Main Requirements	481
Oversight	482
Payment Card Industry Data Security Standard	482
Purpose and Scope	482
Self-Assessment Questionnaire	484
General Data Protection Regulation	484
California Consumer Privacy Act	484
Making Sense of Laws for Information Security Compliance	488

	CHAPTER SUMMARY	489
	KEY CONCEPTS AND TERMS	490
	CHAPTER 15 ASSESSMENT	490
APPENDIX A	Answer Key	493
APPENDIX B	Standard Acronyms	495
APPENDIX C	Earning the CompTIA Security+ Certification	498
	Glossary of Key Terms	501
	References	525
	Index	531

Preface

Purpose of This Text

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

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

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

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

New to This Edition

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

Cloud Labs

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

Learning Features

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

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

Audience

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

Acknowledgments

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

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

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

David Kim

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

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

Michael G. Solomon

The Authors

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

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