INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES

ISSA

Managing Risk in Information Systems

THIRD EDITION

Darril Gibson | Andy Igonor

JONES & BARTLETT
LEARNING

© Jones & Bartlett Learning, LLC. NOT FOR SALE OR DISTRIBUTION.

World Headquarters
Jones & Bartlett Learning
5 Wall Street
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 © 2022 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. *Managing Risk in Information Systems, Third 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.

Production Credits
Math/CS team:
VP, Product Management: Christine Emerton
Director of Product Management: Laura Pagluica
Product Manager: Ned Hinman
Product Specialist/Assistant: Melissa Duffy
Product Coordinator: Paula-Yuan Gregory
Project Manager: Kristen Rogers
Senior Project Specialist: Alex Schab
Senior Digital Project Specialist: Angela Dooley
Marketing Manager: Michael Sullivan
Product Fulfillment Manager: Wendy Kilborn
Composition: Exela Technologies
Development Editor: Ginny Munroe
Technical Editor: Jeff Parker
Cover Design: Briana Yates
Text Design: Briana Yates
Senior Media Development Editor: Troy Liston
Media Development Editor: Faith Brosnan
Rights & Permissions Manager: John Rusk
Rights Specialist: James Fortney
Cover Image (Title Page, Part Opener, Chapter Opener):
© Sai Chan/Shutterstock
Printing and Binding: LSC Communications

Library of Congress Cataloging-in-Publication Data
Library of Congress Cataloging-in-Publication Data unavailable at time of printing.

6048

Printed in the United States of America

24 23 22 21 20   10 9 8 7 6 5 4 3 2 1

© Jones & Bartlett Learning, LLC. NOT FOR SALE OR DISTRIBUTION.

© Sai Chan/Shutterstock

Brief Contents

Preface xix

Acknowledgments xxiii

About the Authors xxv

PART ONE Risk Management Business Challenges 1

CHAPTER 1 Risk Management Fundamentals 3

CHAPTER 2 Managing Risk: Threats, Vulnerabilities, and Exploits 27

CHAPTER 3 Understanding and Maintaining Compliance 55

CHAPTER 4 Developing a Risk Management Plan 83

PART TWO Mitigating Risk 109

CHAPTER 5 Defining Risk Assessment Approaches 111

CHAPTER 6 Performing a Risk Assessment 135

CHAPTER 7 Identifying Assets and Activities to Be Protected 161

CHAPTER 8 Identifying and Analyzing Threats, Vulnerabilities, and Exploits 187

CHAPTER 9 Identifying and Analyzing Risk Mitigation Security Controls 215

CHAPTER 10 Planning Risk Mitigation Throughout an Organization 241

CHAPTER 11 Turning a Risk Assessment into a Risk Mitigation Plan 269

© Jones & Bartlett Learning, LLC. NOT FOR SALE OR DISTRIBUTION.

PART THREE Risk Mitigation Plans 297

CHAPTER 12 Mitigating Risk with a Business Impact Analysis 299

CHAPTER 13 Mitigating Risk with a Business Continuity Plan 323

CHAPTER 14 Mitigating Risk with a Disaster Recovery Plan 349

CHAPTER 15 Mitigating Risk with a Computer Incident Response Team Plan 377

APPENDIX A Answer Key 405

APPENDIX B Standard Acronyms 407

Glossary of Key Terms 411

References 423

Index 427

© Jones & Bartlett Learning, LLC. NOT FOR SALE OR DISTRIBUTION.

© Sai Chan/Shutterstock

Contents

Preface xix

Acknowledgments xxiii

About the Authors xxv

PART ONE **Risk Management Business Challenges** 1

CHAPTER 1 **Risk Management Fundamentals** 3

What Is Risk? 4

Compromise of Business Functions 5
Threats, Vulnerabilities, Assets, and Impact 6

Classify Business Risks 9

Risks Posed by People 10
Risks Posed by a Lack of Process 11
Risks Posed by Technology 12

Risk Identification Techniques 14

Identifying Threats 14
Identifying Vulnerabilities 16
Assessing Impact and Likelihood 17

Risk Management Process 19

Cost-Benefit Analysis 20
Profitability Versus Survivability 21

Risk-Handling Strategies 23

Avoiding 23
Sharing or Transferring 23
Mitigating 23
Accepting 24
Residual Risk 24

CHAPTER SUMMARY 25

KEY CONCEPTS AND TERMS 25

CHAPTER 1 ASSESSMENT 26

© Jones & Bartlett Learning, LLC. NOT FOR SALE OR DISTRIBUTION.

CHAPTER 2 **Managing Risk: Threats, Vulnerabilities, and Exploits** 27

Understanding and Protecting Assets 28

Understanding and Managing Threats 28

Uncontrollable Nature of Threats 29
Unintentional Threats 29
Intentional Threats 30
Best Practices for Managing Risk Within an IT Infrastructure 32
EY Global Information Security Survey 2018–2019 33

Understanding and Managing Vulnerabilities 34

Threat/Vulnerability Pairs 34
Vulnerabilities Can Be Mitigated 35
Mitigation Techniques 35
Best Practices for Managing Vulnerabilities Within an IT Infrastructure 39

Understanding and Managing Exploits 39

What Is an Exploit? 39
How Do Perpetrators Initiate an Exploit? 42
Where Do Perpetrators Find Information About Vulnerabilities and Exploits? 44
Mitigation Techniques 45
Best Practices for Managing Exploits Within an IT Infrastructure 46

U.S. Federal Government Risk Management Initiatives 46

National Institute of Standards and Technology 47
Department of Homeland Security 49
National Cybersecurity and Communications Integration Center 49
U.S. Computer Emergency Readiness Team 49
The MITRE Corporation and the CVE List 50

CHAPTER SUMMARY 52

KEY CONCEPTS AND TERMS 53

CHAPTER 2 ASSESSMENT 53

CHAPTER 3 **Understanding and Maintaining Compliance** 55

U.S. Compliance Laws 56

Federal Information Security Modernization Act 57
Health Insurance Portability and Accountability Act 57
Gramm-Leach-Bliley Act 60
Sarbanes-Oxley Act 60
Family Educational Rights and Privacy Act 60
Children’s Internet Protection Act 61
Children’s Online Privacy Protection Act 61

Regulations Related to Compliance 62

Securities and Exchange Commission 63
Federal Deposit Insurance Corporation 63
Department of Homeland Security 63
Federal Trade Commission 64

© Jones & Bartlett Learning, LLC. NOT FOR SALE OR DISTRIBUTION.

State Attorney General 65
U.S. Attorney General 65

Organizational Policies for Compliance 66

Standards and Guidelines for Compliance 67

Payment Card Industry Data Security Standard 67
National Institute of Standards and Technology 69
Generally Accepted Information Security Principles 70
Control Objectives for Information and Related Technology 70
International Organization for Standardization 72
International Electrotechnical Commission 73
Information Technology Infrastructure Library 74
Capability Maturity Model Integration 76
General Data Protection Regulation 77
Department of Defense Information Assurance Certification and Accreditation Process 78

CHAPTER SUMMARY 79

KEY CONCEPTS AND TERMS 79

CHAPTER 3 ASSESSMENT 80

CHAPTER 4 Developing a Risk Management Plan 83

Objectives of a Risk Management Plan 84

Objectives Example: Website 85
Objectives Example: HIPAA Compliance 86

Scope of a Risk Management Plan 87

Scope Example: Website 88
Scope Example: HIPAA Compliance 89

Assigning Responsibilities 89

Responsibilities Example: Website 90
Responsibilities Example: HIPAA Compliance 90

Describing Procedures and Schedules for Accomplishment 92

Procedures Example: Website 93
Procedures Example: HIPAA Compliance 93

Reporting Requirements 94

Presenting Recommendations 94
Documenting Management Response to Recommendations 99
Documenting and Tracking Implementation of Accepted Recommendations 99

Plan of Action and Milestones 100

Charting the Progress of a Risk Management Plan 102

Milestone Plan Chart 102
Gantt Chart 103
Critical Path Chart 104

Steps of the NIST Risk Management Framework 104

© Jones & Bartlett Learning, LLC. NOT FOR SALE OR DISTRIBUTION.

CHAPTER SUMMARY 105
KEY CONCEPTS AND TERMS 105
CHAPTER 4 ASSESSMENT 106

PART TWO Mitigating Risk 109

CHAPTER 5 Defining Risk Assessment Approaches 111

Understanding Risk Assessments 112
Importance of Risk Assessments 113
Purpose of a Risk Assessment 113
Critical Components of a Risk Assessment 114
Identifying Scope 114
Identifying Critical Areas 115
Identifying Team Members 116
Types of Risk Assessments 116
Quantitative Risk Assessments 116
Qualitative Risk Assessments 119
Comparing Quantitative and Qualitative Risk Assessments 126
Risk Assessment Challenges 127
Using a Static Process to Evaluate a Moving Target 127
Availability of Resources and Data 128
Data Consistency 129
Estimating Impact Effects 130
Providing Results That Support Resource Allocation and Risk Acceptance 131
Best Practices for Risk Assessment 132
CHAPTER SUMMARY 133
KEY CONCEPTS AND TERMS 133
CHAPTER 5 ASSESSMENT 133

CHAPTER 6 Performing a Risk Assessment 135

Selecting a Risk Assessment Methodology 136
Defining the Assessment 137
Reviewing Previous Findings 139
Identifying the Management Structure 140
Identifying Assets and Activities Within Risk Assessment Boundaries 141
System Access and Availability 142
System Functions 142
Hardware and Software Assets 144
Personnel Assets 144

© Jones & Bartlett Learning, LLC. NOT FOR SALE OR DISTRIBUTION.

Data and Information Assets 144
Facilities and Supplies 145

Identifying and Evaluating Relevant Threats 145

Reviewing Historical Data 146
Performing Threat Modeling 146

Identifying and Evaluating Relevant Vulnerabilities 147

Vulnerability Assessments 147
Exploit Assessments 148

Identifying and Evaluating Controls 149

In-Place and Planned Controls 149
Control Categories 149

Selecting a Methodology Based on Assessment Needs 152

Quantitative Method 153
Qualitative Method 154

Developing Mitigating Recommendations 155

Threat/Vulnerability Pairs 155
Estimate of Cost and Time to Implement 155
Estimate of Operational Impact 156
Cost-Benefit Analysis 157

Presenting Risk Assessment Results 157

Best Practices for Performing Risk Assessments 157

CHAPTER SUMMARY 158

KEY CONCEPTS AND TERMS 159

CHAPTER 6 ASSESSMENT 159

CHAPTER 7 **Identifying Assets and Activities to Be Protected 161**

System Access and Availability 162

System Functions: Manual and Automated 164

Manual Methods 164
Automated Methods 165

Hardware Assets 166

Software Assets 167

Personnel Assets 169

Data and Information Assets 169

Organization 171
Customer 172
Intellectual Property 172
Data Warehousing and Data Mining 173

© Jones & Bartlett Learning, LLC. NOT FOR SALE OR DISTRIBUTION.

Asset and Inventory Management Within the Seven Domains of a Typical IT Infrastructure 175

User Domain 176
Workstation Domain 176
LAN Domain 177
LAN-to-WAN Domain 177
WAN Domain 178
Remote Access Domain 178
System/Application Domain 178

Identifying Facilities and Supplies Needed to Maintain Business Operations 179

Mission-Critical Systems and Applications Identification 179
Business Impact Analysis Planning 180
Business Continuity Planning 181
Disaster Recovery Planning 182
Business Liability Insurance Planning 183
Asset Replacement Insurance Planning 183

CHAPTER SUMMARY 184

KEY CONCEPTS AND TERMS 184

CHAPTER 7 ASSESSMENT 184

CHAPTER 8 **Identifying and Analyzing Threats, Vulnerabilities, and Exploits 187**

Threat Assessments 188

Techniques for Identifying Threats 191
Best Practices for Threat Assessments Within the Seven Domains of a Typical IT Infrastructure 194

Vulnerability Assessments 195

Review of Documentation 197
Review of System Logs, Audit Trails, and Intrusion Detection and Prevention System Outputs 198
Vulnerability Scans and Other Assessment Tools 199
Audits and Personnel Interviews 200
Process Analysis and Output Analysis 201
System Testing 202
Best Practices for Performing Vulnerability Assessments Within the Seven Domains of a Typical IT Infrastructure 205

Exploit Assessments 206

Identifying Exploits 207
Mitigating Exploits with a Gap Analysis and Remediation Plan 210
Implementing Configuration or Change Management 210
Verifying and Validating the Exploit Has Been Mitigated 211
Best Practices for Performing Exploit Assessments Within an IT Infrastructure 211

CHAPTER SUMMARY 212

KEY CONCEPTS AND TERMS 212

CHAPTER 8 ASSESSMENT 212

© Jones & Bartlett Learning, LLC. NOT FOR SALE OR DISTRIBUTION.

CHAPTER 9 Identifying and Analyzing Risk Mitigation Security Controls 215

In-Place Controls 216

Planned Controls 216

Control Categories 217
NIST Control Families 217

Procedural Control Examples 220

Policies and Procedures 220
Security Plans 222
Insurance and Bonding 223
Background and Financial Checks 224
Data Loss Prevention Program 225
Education, Training, and Awareness 225
Rules of Behavior 226
Software Testing 227

Technical Control Examples 227

Logon Identifier 228
Session Time-Out 228
System Logs and Audit Trails 229
Data Range and Reasonableness Checks 229
Firewalls and Routers 230
Encryption 232
Public Key Infrastructure 233

Physical Control Examples 235

Locked Doors, Guards, Access Logs, and Closed-Circuit Television 235
Fire Detection and Suppression 236
Water Detection 237
Temperature and Humidity Detection 237
Electrical Grounding and Circuit Breakers 238

Best Practices for Risk Mitigation Security Controls 239

CHAPTER SUMMARY 239

KEY CONCEPTS AND TERMS 239

CHAPTER 9 ASSESSMENT 240

CHAPTER 10 Planning Risk Mitigation Throughout an Organization 241

Where Should an Organization Start with Risk Mitigation? 242

What Is the Scope of Risk Management for an Organization? 243

Critical Business Operations 244
Customer Service Delivery 245
Mission-Critical Business Systems, Applications, and Data Access 246
Seven Domains of a Typical IT Infrastructure 249
Information Systems Security Gap 252

Understanding and Assessing the Impact of Legal and Compliance Issues on an Organization 253

© Jones & Bartlett Learning, LLC. NOT FOR SALE OR DISTRIBUTION.

Legal Requirements, Compliance Laws, Regulations, and Mandates 255
Assessing the Impact of Legal and Compliance Issues on an Organization's Business Operations 257

Translating Legal and Compliance Implications for an Organization 261

Assessing the Impact of Legal and Compliance Implications on the Seven Domains of a Typical IT Infrastructure 261

Assessing How Security Countermeasures, Controls, and Safeguards Can Assist With Risk Mitigation 262

Understanding the Operational Implications of Legal and Compliance Requirements 263

Identifying Risk Mitigation and Risk Reduction Elements for the Entire Organization 263

Performing a Cost-Benefit Analysis 264

Best Practices for Planning Risk Mitigation Throughout an Organization 265

CHAPTER SUMMARY 266

KEY CONCEPTS AND TERMS 266

CHAPTER 10 ASSESSMENT 267

CHAPTER 11 Turning a Risk Assessment into a Risk Mitigation Plan 269

Reviewing the Risk Assessment for the IT Infrastructure 270

Overlapping Countermeasures 271
Risk Assessments: Understanding Threats and Vulnerabilities 272
Identifying Countermeasures 273

Translating a Risk Assessment into a Risk Mitigation Plan 276

Cost to Implement 276
Time to Implement 280
Operational Impact 283

Prioritizing Risk Elements That Require Risk Mitigation 283

Using a Threat Likelihood/Impact Matrix 284
Prioritizing Countermeasures 284

Verifying Risk Elements and How They Can Be Mitigated 286

Performing a Cost-Benefit Analysis on the Identified Risk Elements 287

Calculating the CBA 287
A CBA Report 288

Implementing a Risk Mitigation Plan 289

Staying Within Budget 289
Staying on Schedule 290

Following Up on the Risk Mitigation Plan 292

Ensuring Countermeasures Have Been Implemented 293
Ensuring Security Gaps Have Been Closed 293

© Jones & Bartlett Learning, LLC. NOT FOR SALE OR DISTRIBUTION.

Best Practices for Enabling a Risk Mitigation Plan from the Risk Assessment 294

CHAPTER SUMMARY 295

KEY CONCEPTS AND TERMS 295

CHAPTER 11 ASSESSMENT 296

PART THREE Risk Mitigation Plans 297

CHAPTER 12 Mitigating Risk with a Business Impact Analysis 299

What Is a Business Impact Analysis? 300

Collecting Data 301
Varying Data Collection Methods 302

Defining the Scope of the Business Impact Analysis 302

Objectives of a Business Impact Analysis 304

Identifying Critical Business Functions 305
Identifying Critical Resources 306
Identifying the MAO and Impact 308
Identifying Recovery Requirements 310

Steps of a Business Impact Analysis Process 312

Identifying the Environment 313
Identifying Stakeholders 313
Identifying Critical Business Functions 314
Identifying Critical Resources 314
Identifying the MAO 315
Identifying Recovery Priorities 315
Developing the BIA Report 316

Identifying Mission-Critical Business Functions and Processes 317

Mapping Business Functions and Processes to IT Systems 318

Best Practices for Performing a BIA for an Organization 319

CHAPTER SUMMARY 320

KEY CONCEPTS AND TERMS 320

CHAPTER 12 ASSESSMENT 320

CHAPTER 13 Mitigating Risk with a Business Continuity Plan 323

What Is a Business Continuity Plan? 324

Elements of a BCP 325

Purpose 326
Scope 326
Assumptions and Planning Principles 327
System Description and Architecture 329

© Jones & Bartlett Learning, LLC. NOT FOR SALE OR DISTRIBUTION.

Responsibilities 333
Notification and Activation Phase 336
Recovery Phase 339
Reconstitution Phase (Return to Normal Operations) 340
Plan Training, Testing, and Exercises 342
Plan Maintenance 344

How Does a BCP Mitigate an Organization's Risk? 346

Best Practices for Implementing a BCP for an Organization 346

CHAPTER SUMMARY 347

KEY CONCEPTS AND TERMS 347

CHAPTER 13 ASSESSMENT 347

CHAPTER 14 Mitigating Risk with a Disaster Recovery Plan 349

What Is a Disaster Recovery Plan? 350

Need for a DRP 352
Purpose of a DRP 352

Critical Success Factors 352

What Management Must Provide 353
What DRP Developers Need 353
Primary Concerns 355
Disaster Recovery Financial Budget 362

Elements of a DRP 362

Purpose 363
Scope 364
Disaster/Emergency Declaration 365
Communications 365
Emergency Response 366
Activities 366
Recovery Procedures 367
Critical Operations, Customer Service, and Operations Recovery 369
Restoration and Normalization 370
Testing 370
Maintenance and DRP Update 371

How Does a DRP Mitigate an Organization's Risk? 372

Best Practices for Implementing a DRP for an Organization 372

CHAPTER SUMMARY 374

KEY CONCEPTS AND TERMS 374

CHAPTER 14 ASSESSMENT 374

© Jones & Bartlett Learning, LLC. NOT FOR SALE OR DISTRIBUTION.

CHAPTER 15 **Mitigating Risk with a Computer Incident Response Team Plan 377**

What Is a Computer Incident Response Team Plan? 378

Purpose of a CIRT Plan 379

Elements of a CIRT Plan 381

CIRT Members 381
CIRT Policies 385
Incident Handling Process 386
Communication Escalation Procedures 394
Incident Handling Procedures 395

How Does a CIRT Plan Mitigate an Organization's Risk? 400

Best Practices for Implementing a CIRT Plan for an Organization 400

CHAPTER SUMMARY 401

KEY CONCEPTS AND TERMS 401

CHAPTER 15 ASSESSMENT 402

APPENDIX A **Answer Key 405**

APPENDIX B **Standard Acronyms 407**

Glossary of Key Terms 411

References 423

Index 427

© Jones & Bartlett Learning, LLC. NOT FOR SALE OR DISTRIBUTION.

© Jones & Bartlett Learning, LLC. NOT FOR SALE OR DISTRIBUTION.

To my wife, who has enriched my life in so many ways over the past 22 years.
I'm looking forward to sharing many more with you.

—Darril Gibson

To my wife and our boys, for their patience and support.

—Andy Igonor

© Jones & Bartlett Learning, LLC. NOT FOR SALE OR DISTRIBUTION.

© Jones & Bartlett Learning, LLC. NOT FOR SALE OR DISTRIBUTION.

© Sai Chan/Shutterstock

Preface

Purpose of This Book

This book is part of the Information Systems Security & Assurance Series from Jones & Bartlett Learning (https://www.jblearning.com/cybersecurity/issa). 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. The books in this series deliver fundamental information security principles packed with real-world applications and examples. Authored by Certified Information Systems Security Professionals (CISSPs), they deliver comprehensive information on all aspects of information security. Reviewed word for word by leading technical experts in the field, these books are not just current, but also forward thinking, putting you in the position to solve the cybersecurity challenges not just of today, but of tomorrow as well.

This book provides a comprehensive view of managing risk in information systems. It covers the fundamentals of risk and risk management and includes in-depth details on more comprehensive risk management topics in three major parts.

Part One, Risk Management Business Challenges, addresses many of the issues relevant to present-day businesses. It covers details of risks, threats, and vulnerabilities. Topics help students understand the importance of risk management in the organization, including many of the techniques used to manage risks. Several current laws are presented with clear descriptions of how they are relevant in organizations. It also includes a chapter describing the contents of a risk management plan.

Part Two, Mitigating Risk, focuses on risk assessments. Topics presented include risk assessment approaches, including the overall steps in performing a risk assessment. It covers the importance of identifying assets and then identifying potential threats, vulnerabilities, and exploits against these assets. Chapter 9 covers the types of controls that can be used to mitigate risk. The last two chapters in this part identify how to plan risk mitigation throughout the organization and convert the risk assessment into a risk management plan.

Part Three, Risk Mitigation Plans, covers the many elements of risk mitigation plans, such as a business impact analysis and a business continuity plan. The last two chapters cover disaster recovery and computer incident response team plans.

© Jones & Bartlett Learning, LLC. NOT FOR SALE OR DISTRIBUTION.

Learning Features

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

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

Audience

The material is suitable for undergraduate or graduate computer science 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.

New to This Edition

This text has been broadly updated to include new and emerging concepts in the expanding field of information systems and cybersecurity, in particular risk management. Concepts are more appropriately defined and explained; for example, the definition of *risk* references *assets* as a critical component of the totality of risk. Risk management and assessment topics have been updated throughout the book with references to threat sources, for example, advanced persistent threats. Included are updated references and examples of threat-likelihood impacts and how organizations compute risk loss scenarios. Explanations of business continuity plans, minimum business continuity objectives, disaster recovery plans, and recovery sites are updated. Several new guidelines have been introduced in the text to reflect advances in the field of cybersecurity. In particular, federal guidelines from the National Institute of Standards and Technology (NIST) and the Department of Homeland Security have been updated, with the inclusion of new NIST Special Publications: 800-183; 800-154; 800-153; 800-150; 800-84; 800-63 a, b, and c; 800-53 Rev. 5; 800-34; and 800-37.

The text includes updated references to the current organizational state of affairs in the field of cybersecurity, such as surveys of executives in the field, and references to the new and emerging topics of cloud computing, analytics, mobile computing, artificial intelligence, machine learning, robotic process automation, and blockchain. Besides updated information on the NIST Risk Management Framework, updates to the Common Vulnerabilities and Exposures (CVE) are included. The textbook now has updated references to U.S. and international compliance laws, including the Federal Information Security Modernization Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), and the EU's General Data Protection Regulation (GDPR). The Children's Online Privacy Protection Act (COPPA) is introduced as well as the Equifax data breach. The text

© Jones & Bartlett Learning, LLC. NOT FOR SALE OR DISTRIBUTION.

includes updated references to ISACA's Control Objectives for Information and Related Technologies (COBIT) 2019. Updated end-of-chapter questions are also included in the text.

Cloud Labs

This text is accompanied by Cybersecurity Cloud Labs. These hands-on virtual labs provide immersive mock IT infrastructures whereby students can learn and practice foundational cybersecurity skills as an extension of the lessons in this textbook. For more information or to purchase the labs, visit go.jblearning.com/gibson3e.

© Jones & Bartlett Learning, LLC. NOT FOR SALE OR DISTRIBUTION.

© Jones & Bartlett Learning, LLC. NOT FOR SALE OR DISTRIBUTION.

© Sai Chan/Shutterstock

Acknowledgments

Jones & Bartlett Learning would personally like to thank all the people who reviewed the second edition of this book, whose feedback helped to shape this revision:

Michael D. Barker
Columbus State University

David Barnes
Penn State Altoona

Casey Cegielski
Auburn University

Shaun L. Gray
University of the Cumberlands

Dr. Wendi M. Kappers
Embry-Riddle Aeronautical University

Andrew Mangle
Bowie State University

Francis J. Monaco
Charter Oak State College

Andrew Morrow
Penn State University Harrisburg

Phoebe Tsai
Cedarville University

George J. Trawick
National Defense University

© Jones & Bartlett Learning, LLC. NOT FOR SALE OR DISTRIBUTION.

© Jones & Bartlett Learning, LLC. NOT FOR SALE OR DISTRIBUTION.

© Sai Chan/Shutterstock

About the Authors

Darril Gibson is the CEO of YCDA, LLC (short for You Can Do Anything). He regularly writes and consults on a wide variety of security and technical topics and holds several certifications, including MCSE, MCDBA, MCSD, MCITP, ITIL v3, Security+, SSCP, and CISSP. He has authored or coauthored more than 30 books, including the best-selling *Security+: Get Certified, Get Ahead* series of books, and regularly blogs at http://blogs.getcertifiedgetahead.com.

Andy Igonor currently serves as the director of Academic Programs and the associate dean of Information Technology/Cloud Computing at Western Governor's University. He previously served as the dean of the Ross College of Business at Franklin University. He is an IT professional and entrepreneur with over 20 years of experience spanning several industries, from education to health care and consulting. He has worked and lived in Africa, Asia, Europe, the Middle East, and North America. Andy holds a doctorate in Information Systems from the Bristol Business School, United Kingdom. He also holds several certifications, including Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC), and Certified Professional in Health Information Management and Systems (CPHIMS). He has published several articles in information technology and also coauthored four books.

© Jones & Bartlett Learning, LLC. NOT FOR SALE OR DISTRIBUTION.

© Jones & Bartlett Learning, LLC. NOT FOR SALE OR DISTRIBUTION.