

ISSA

# Fundamentals of Information Systems Security

THIRD EDITION

---

David Kim | Michael G. Solomon

ISSA

# Fundamentals of Information Systems Security

THIRD EDITION

David Kim | Michael G. Solomon



JONES & BARTLETT  
LEARNING

World Headquarters  
Jones & Bartlett Learning  
5 Wall Street  
Burlington, MA 01803  
978-443-5000  
info@jblearning.com  
www.jblearning.com

Jones and Bartlett's books and products are available through most bookstores and online booksellers. To contact Jones and Bartlett Publishers directly, call 800-832-0034, fax 978-443-8000, or visit our website [www.jbpub.com](http://www.jbpub.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](mailto:specialsales@jblearning.com).

Copyright © 2018 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, 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**

VP, Executive Publisher: David D. Cella  
Executive Editor: Matt Kane  
Acquisitions Editor: Laura Pagluica  
Editorial Assistant: Mary Menzemer  
Production Manager: Carolyn Rogers Pershouse  
Associate Production Editor: Juna Abrams  
Director of Marketing: Andrea DeFronzo  
Marketing Manager: Amy Langlais  
Manufacturing and Inventory Control Supervisor: Amy Bacus

Composition: S4Carlisle Publishing Services  
Cover Design: Scott Moden  
Director of Rights & Media: Joanna Gallant  
Rights & Media Specialist: Merideth Tumas  
Media Development Editor: Shannon Sheehan  
Cover and Header Image: © Zffoto/Shutterstock  
Printing and Binding: Edwards Brothers Malloy  
Cover Printing: Edwards Brothers Malloy

#### **Library of Congress Cataloging-in-Publication Data**

Names: Kim, David (Information technology security consultant), author. | Solomon, Michael (Michael G.), 1963- author.  
Title: Fundamentals of information systems security / David Kim and Michael G. Solomon.  
Description: Third edition. | Burlington, Massachusetts : Jones & Bartlett Learning, 2016. | Includes bibliographical references and index.  
Identifiers: LCCN 2016038356 | ISBN 9781284116458 (pbk.)  
Subjects: LCSH: Computer security. | Information resources--Security measures.  
Classification: LCC QA76.9.A25 K536 2016 | DDC 005.8--dc23  
LC record available at <https://lccn.loc.gov/2016038356>

6048

Printed in the United States of America  
20 19 18 17 16 10 9 8 7 6 5 4 3 2 1

*This book is dedicated to our readers, students, and 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 privacy data of our citizens.*

*—David Kim*

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

*—Michael G. Solomon*



# Contents

<b>Preface</b>	<b>xix</b>
<b>Acknowledgments</b>	<b>xxi</b>
<b>The Authors</b>	<b>xxi</b>

## **PART I**

### **The Need for Information Security 1**

#### **CHAPTER 1**

#### **Information Systems Security 2**

##### **Information Systems Security 3**

Risks, Threats, and Vulnerabilities 11

What Is Information Systems Security? 12

U.S. Compliance Laws Drive Need for Information Systems Security 12

##### **Tenets of Information Systems Security 14**

Confidentiality 16

Integrity 17

Availability 17

##### **The Seven Domains of a Typical IT Infrastructure 19**

User Domain 19

Workstation Domain 22

LAN Domain 22

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 38**

Ethics and the Internet 40

##### **IT Security Policy Framework 40**

Definitions 41

Foundational IT Security Policies 41

##### **Data Classification Standards 42**

##### **CHAPTER SUMMARY 44**

##### **KEY CONCEPTS AND TERMS 44**

##### **CHAPTER 1 ASSESSMENT 45**

**CHAPTER 2****The Internet of Things Is Changing How We Live 47****Evolution of the Internet of Things 49****Converting to a TCP/IP World 50****IoT's Impact on Human and Business Life 51**

How People Like to Communicate 52

IoT Applications That Impact Our Lives 52

**Evolution from Bricks and Mortar to E-Commerce 55****Why Businesses Must Have an Internet  
and IoT Marketing Strategy 57****IP Mobility 58**

Mobile Users and Bring Your Own Device 58

**Mobile Applications 59**

IP Mobile Communications 60

**New Challenges Created by the IoT 62**

Security 62

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****Malicious Attacks, Threats, and Vulnerabilities 72****Malicious Activity on the Rise 73****What Are You Trying to Protect? 74**

Customer Data 74

IT and Network Infrastructure 75

Intellectual Property 76

Finances and Financial Data 76

Service Availability and Productivity 77

Reputation 78

**Whom Are You Trying to Catch? 78****Attack Tools 79**

Protocol Analyzers 80

Port Scanners 80

OS Fingerprint Scanners 80

Vulnerability Scanners 80

Exploit Software 81

Wardialers 81

Password Crackers	82
Keystroke Loggers	82
<b>What Is a Security Breach?</b>	<b>83</b>
Denial of Service Attacks	83
Distributed Denial of Service Attacks	84
Unacceptable Web Browsing	84
Wiretapping	85
Backdoors	85
Data Modifications	86
Additional Security Challenges	86
<b>What Are Risks, Threats, and Vulnerabilities?</b>	<b>88</b>
Threat Targets	89
Threat Types	90
<b>What Is a Malicious Attack?</b>	<b>92</b>
Birthday Attacks	93
Brute-Force Password Attacks	93
Dictionary Password Attacks	94
IP Address Spoofing	94
Hijacking	94
Replay Attacks	95
Man-in-the-Middle Attacks	95
Masquerading	96
Eavesdropping	96
Social Engineering	96
Phreaking	97
Phishing	97
Pharming	98
<b>What Is Malicious Software?</b>	<b>99</b>
Viruses	99
Worms	100
Trojan Horses	100
Rootkits	101
Spyware	101
<b>What Are Common Types of Attacks?</b>	<b>102</b>
Social Engineering Attacks	103
Wireless Network Attacks	104
Web Application Attacks	104
<b>What Is a Countermeasure?</b>	<b>106</b>
Countering Malware	106
Protecting Your System with Firewalls	108
<b>CHAPTER SUMMARY</b>	<b>108</b>
<b>KEY CONCEPTS AND TERMS</b>	<b>109</b>
<b>CHAPTER 3 ASSESSMENT</b>	<b>110</b>



<b>CHAPTER 4</b>	<b>The Drivers of the Information Security Business</b>	<b>112</b>
	<b>Defining Risk Management</b>	<b>113</b>
	<b>Implementing a BIA, a BCP, and a DRP</b>	<b>115</b>
	Business Impact Analysis	115
	Business Continuity Plan	116
	Disaster Recovery Plan	118
	<b>Assessing Risks, Threats, and Vulnerabilities</b>	<b>122</b>
	<b>Closing the Information Security Gap</b>	<b>123</b>
	<b>Adhering to Compliance Laws</b>	<b>124</b>
	<b>Keeping Private Data Confidential</b>	<b>127</b>
	<b>Mobile Workers and Use of Personally Owned Devices</b>	<b>129</b>
	BYOD Concerns	129
	Endpoint and Device Security	130
	<b>CHAPTER SUMMARY</b>	<b>131</b>
	<b>KEY CONCEPTS AND TERMS</b>	<b>132</b>
	<b>CHAPTER 4 ASSESSMENT</b>	<b>132</b>
<b>PART II</b>	<b>Securing Today's Information Systems</b>	<b>135</b>
<b>CHAPTER 5</b>	<b>Access Controls</b>	<b>136</b>
	<b>Four-Part Access Control</b>	<b>137</b>
	<b>Two Types of Access Controls</b>	<b>138</b>
	Physical Access Control	138
	Logical Access Control	138
	<b>Authorization Policies</b>	<b>140</b>
	<b>Methods and Guidelines for Identification</b>	<b>141</b>
	Identification Methods	141
	Identification Guidelines	141
	<b>Processes and Requirements for Authentication</b>	<b>142</b>
	Authentication Types	142
	Single Sign-On	151
	<b>Policies and Procedures for Accountability</b>	<b>154</b>
	Log Files	154
	Monitoring and Reviews	154
	Data Retention, Media Disposal, and Compliance Requirements	154
	<b>Formal Models of Access Control</b>	<b>156</b>
	Discretionary Access Control	157
	Operating Systems-Based DAC	157

Mandatory Access Control	159
Nondiscretionary Access Control	160
Rule-Based Access Control	160
Access Control Lists	160
Role-Based Access Control	161
Content-Dependent Access Control	163
Constrained User Interface	163
Other Access Control Models	164
<b>Effects of Breaches in Access Control</b>	<b>166</b>
<b>Threats to Access Controls</b>	<b>167</b>
<b>Effects of Access Control Violations</b>	<b>168</b>
<b>Credential and Permissions Management</b>	<b>169</b>
<b>Centralized and Decentralized Access Control</b>	<b>169</b>
Types of AAA Servers	169
Decentralized Access Control	172
Privacy	172
<b>CHAPTER SUMMARY</b>	<b>177</b>
<b>KEY CONCEPTS AND TERMS</b>	<b>177</b>
<b>CHAPTER 5 ASSESSMENT</b>	<b>178</b>

**CHAPTER 6**

<b>Security Operations and Administration</b>	<b>181</b>
<b>Security Administration</b>	<b>182</b>
Controlling Access	182
Documentation, Procedures, and Guidelines	183
Disaster Assessment and Recovery	183
Security Outsourcing	184
<b>Compliance</b>	<b>185</b>
Event Logs	186
Compliance Liaison	186
Remediation	186
<b>Professional Ethics</b>	<b>187</b>
Common Fallacies About Ethics	187
Codes of Ethics	188
Personnel Security Principles	189
<b>The Infrastructure for an IT Security Policy</b>	<b>192</b>
Policies	192
Standards	194
Procedures	194
Baselines	195
Guidelines	196

<b>Data Classification Standards</b>	<b>196</b>
Information Classification Objectives	197
Examples of Classification	197
Classification Procedures	197
Assurance	198
<b>Configuration Management</b>	<b>199</b>
Hardware Inventory and Configuration Chart	199
<b>The Change Management Process</b>	<b>200</b>
Change Control Management	200
Change Control Committees	201
Change Control Procedures	202
Change Control Issues	203
<b>Application Software Security</b>	<b>203</b>
The System Life Cycle	203
Testing Application Software	205
<b>Software Development and Security</b>	<b>208</b>
Software Development Models	209
<b>CHAPTER SUMMARY</b>	<b>212</b>
<b>KEY CONCEPTS AND TERMS</b>	<b>213</b>
<b>CHAPTER 6 ASSESSMENT</b>	<b>213</b>
<b>Auditing, Testing, and Monitoring</b>	<b>216</b>
<b>Security Auditing and Analysis</b>	<b>217</b>
Security Controls Address Risk	218
Determining What Is Acceptable	219
Permission Levels	219
Areas of Security Audits	220
Purpose of Audits	220
Customer Confidence	221
<b>Defining Your Audit Plan</b>	<b>223</b>
Defining the Scope of the Plan	223
<b>Auditing Benchmarks</b>	<b>224</b>
<b>Audit Data Collection Methods</b>	<b>226</b>
Areas of Security Audits	226
Control Checks and Identity Management	227
<b>Post-Audit Activities</b>	<b>228</b>
Exit Interview	228
Data Analysis	228
Generation of Audit Report	228
Presentation of Findings	229

**CHAPTER 7**

<b>Security Monitoring</b>	<b>229</b>
Security Monitoring for Computer Systems	230
Monitoring Issues	231
Logging Anomalies	232
Log Management	232
<b>Types of Log Information to Capture</b>	<b>233</b>
<b>How to Verify Security Controls</b>	<b>234</b>
Intrusion Detection System (IDS)	234
Analysis Methods	236
HIDS	237
Layered Defense: Network Access Control	237
Control Checks: Intrusion Detection	238
Host Isolation	238
System Hardening	238
Review Antivirus Programs	241
<b>Monitoring and Testing Security Systems</b>	<b>241</b>
Monitoring	241
Testing	241
<b>CHAPTER SUMMARY</b>	<b>249</b>
<b>KEY CONCEPTS AND TERMS</b>	<b>249</b>
<b>CHAPTER 7 ASSESSMENT</b>	<b>249</b>

**CHAPTER 8**

<b>Risk, Response, and Recovery</b>	<b>251</b>
<b>Risk Management and Information Security</b>	<b>252</b>
Risk Terminology	253
Elements of Risk	254
Purpose of Risk Management	254
<b>The Risk Management Process</b>	<b>255</b>
Identify Risks	256
Assess Risks	259
Plan a Risk Response	263
Implement the Risk Response Plan	265
Monitor and Control Risk Response	269
<b>Business Continuity Management</b>	<b>270</b>
Terminology	271
Assessing Maximum Tolerable Downtime	272
Business Impact Analysis	273
Plan Review	274
Testing the Plan	274
<b>Backing Up Data and Applications</b>	<b>276</b>
Types of Backups	276

**Incident Handling 277**

Preparation	278
Identification	278
Notification	278
Response	279
Recovery	280
Followup	280
Documentation and Reporting	280

**Recovery from a Disaster 280**

Activating the Disaster Recovery Plan	281
Operating in a Reduced/Modified Environment	281
Restoring Damaged Systems	282
Disaster Recovery Issues	282
Recovery Alternatives	282
Interim or Alternate Processing Strategies	283

**CHAPTER SUMMARY 285****KEY CONCEPTS AND TERMS 286****CHAPTER 8 ASSESSMENT 287****CHAPTER 9****Cryptography 288****What Is Cryptography? 289**

Basic Cryptographic Principles	290
A Brief History of Cryptography	291
Cryptography's Role in Information Security	292

**Business and Security Requirements for Cryptography 295**

Internal Security	295
Security in Business Relationships	295
Security Measures That Benefit Everyone	296

**Cryptographic Principles, Concepts, and Terminology 296**

Cryptographic Functions and Ciphers	296
-------------------------------------	-----

**Types of Ciphers 299**

Transposition Ciphers	300
Substitution Ciphers	300
Product and Exponentiation Ciphers	302

**Symmetric and Asymmetric Key Cryptography 303**

Symmetric Key Ciphers	303
Asymmetric Key Ciphers	304
Cryptanalysis and Public Versus Private Keys	305

**Keys, Keyspace, and Key Management 308**

Cryptographic Keys and Keyspace	308
Key Management	309
Key Distribution	310
Key Distribution Centers	310

<b>Digital Signatures and Hash Functions</b>	<b>311</b>
Hash Functions	311
Digital Signatures	311
<b>Cryptographic Applications and Uses in Information System Security</b>	<b>312</b>
Other Cryptographic Tools and Resources	313
Symmetric Key Standards	314
Asymmetric Key Solutions	316
Hash Function and Integrity	318
Digital Signatures and Nonrepudiation	320
<b>Principles of Certificates and Key Management</b>	<b>321</b>
Modern Key Management Techniques	321
<b>CHAPTER SUMMARY</b>	<b>323</b>
<b>KEY CONCEPTS AND TERMS</b>	<b>324</b>
<b>CHAPTER 9 ASSESSMENT</b>	<b>324</b>

**CHAPTER 10**

<b>Networks and Telecommunications</b>	<b>326</b>
<b>The Open Systems Interconnection Reference Model</b>	<b>327</b>
<b>The Main Types of Networks</b>	<b>329</b>
Wide Area Networks	329
Local Area Networks	332
<b>TCP/IP and How It Works</b>	<b>334</b>
TCP/IP Overview	334
IP Addressing	335
Common Ports	336
Common Protocols	336
Internet Control Message Protocol	336
<b>Network Security Risks</b>	<b>338</b>
Categories of Risk	338
<b>Basic Network Security Defense Tools</b>	<b>341</b>
Firewalls	341
Virtual Private Networks and Remote Access	345
Network Access Control	347
<b>Wireless Networks</b>	<b>347</b>
Wireless Access Points	348
Wireless Network Security Controls	348
<b>CHAPTER SUMMARY</b>	<b>351</b>
<b>KEY CONCEPTS AND TERMS</b>	<b>351</b>
<b>CHAPTER 10 ASSESSMENT</b>	<b>352</b>

**CHAPTER 11****Malicious Code and Activity 354****Characteristics, Architecture,  
and Operations of Malicious Software 355****The Main Types of Malware 356**

Virus	356
Spam	363
Worms	364
Trojan Horses	366
Logic Bombs	367
Active Content Vulnerabilities	367
Malicious Add-Ons	367
Injection	368
Botnets	369
Denial of Service Attacks	369
Spyware	371
Adware	372
Phishing	372
Keystroke Loggers	373
Hoaxes and Myths	373
Homepage Hijacking	374
Webpage Defacements	374

**A Brief History of Malicious Code Threats 375**

1970s and Early 1980s: Academic Research and UNIX	375
1980s: Early PC Viruses	376
1990s: Early LAN Viruses	376
Mid-1990s: Smart Applications and the Internet	377
2000 to Present	377

**Threats to Business Organizations 378**

Types of Threats	378
Internal Threats from Employees	379

**Anatomy of an Attack 379**

What Motivates Attackers?	380
The Purpose of an Attack	380
Types of Attacks	380
Phases of an Attack	382

**Attack Prevention Tools and Techniques 387**

Application Defenses	388
Operating System Defenses	388
Network Infrastructure Defenses	389
Safe Recovery Techniques and Practices	390
Implementing Effective Software Best Practices	390

**Intrusion Detection Tools and Techniques 390**

Antivirus Scanning Software	391
Network Monitors and Analyzers	391

Content/Context Filtering and Logging Software	391
Honeypots and Honeynets	392

**CHAPTER SUMMARY 393**

**KEY CONCEPTS AND TERMS 393**

**CHAPTER 11 ASSESSMENT 393**

**PART III Information Security Standards, Education, Certifications, and Laws 395**

**CHAPTER 12**

**Information Security Standards 396**

**Standards Organizations 397**

National Institute of Standards and Technology	397
International Organization for Standardization	398
International Electrotechnical Commission	400
World Wide Web Consortium	401
Internet Engineering Task Force	401
Institute of Electrical and Electronics Engineers	403
International Telecommunication Union Telecommunication Sector	404
American National Standards Institute	405
European Telecommunications Standards Institute	
Cyber Security Technical Committee	406

**ISO 17799 (Withdrawn) 407**

ISO/IEC 27002	408
---------------	-----

**Payment Card Industry Data Security Standard 409**

**CHAPTER SUMMARY 410**

**KEY CONCEPTS AND TERMS 411**

**CHAPTER 12 ASSESSMENT 411**

**CHAPTER 13**

**Information Systems Security Education and Training 412**

**Self-Study Programs 413**

**Instructor-Led Programs 416**

Certificate Programs	416
Continuing Education Programs	418

**Postsecondary Degree Programs 419**

Associate's Degree	420
Bachelor's Degree	420
Master of Science Degree	421
Master of Business Administration	423
Doctoral Degree	424



**Information Security Training Programs 425**

Security Training Requirements	426
Security Training Organizations	427
Security Awareness Training	428

**CHAPTER SUMMARY 430****KEY CONCEPTS AND TERMS 430****CHAPTER 13 ASSESSMENT 431****CHAPTER 14****Information Security Professional Certifications 433****U.S. Department of Defense/Military Directive 8570.01 434**

U.S. DoD/Military Directive 8140	434
U.S. DoD/NSA Training Standards	436

**Vendor-Neutral Professional Certifications 437**

International Information Systems Security Certification Consortium, Inc.	438
SSCP®	438
CISSP®	438
CAP®	439
CSSLP®	439
CCFP®	439
HCISPP®	439
CCSP®	440

Additional (ISC)<sup>2</sup> Professional Certifications 440

Global Information Assurance Certification/SANS Institute 440

Certified Internet Webmaster 441

CompTIA 441

ISACA® 443

Other Information Systems Security Certifications 443

**Vendor-Specific Professional Certifications 443**

Cisco Systems 444

**Juniper Networks 447**

RSA 447

Symantec 447

Check Point 449

**CHAPTER SUMMARY 449****KEY CONCEPTS AND TERMS 450****CHAPTER 14 ASSESSMENT 450****CHAPTER 15****U.S. Compliance Laws 452****Compliance Is the Law 453****Federal Information Security 456**

The Federal Information Security Management Act of 2002 456

The Federal Information Security Modernization Act of 2014 458

The Role of the National Institute of Standards and Technology	459
National Security Systems	461
<b>The Health Insurance Portability and Accountability Act</b>	<b>461</b>
Purpose and Scope	461
Main Requirements of the HIPAA Privacy Rule	462
Main Requirements of the HIPAA Security Rule	464
Oversight	464
Omnibus Regulations	466
<b>The Gramm-Leach-Bliley Act</b>	<b>467</b>
Purpose and Scope	469
Main Requirements of the GLBA Privacy Rule	470
Main Requirements of the GLBA Safeguards Rule	471
Oversight	472
<b>The Sarbanes-Oxley Act</b>	<b>472</b>
Purpose and Scope	473
SOX Control Certification Requirements	473
SOX Records Retention Requirements	475
Oversight	475
<b>The Family Educational Rights and Privacy Act</b>	<b>476</b>
Purpose and Scope	476
Main Requirements	477
Oversight	478
<b>The Children's Internet Protection Act</b>	<b>478</b>
Purpose and Scope	478
Main Requirements	479
Oversight	480
<b>Payment Card Industry Data Security Standard</b>	<b>480</b>
Purpose and Scope	481
Self-Assessment Questionnaire	481
Main Requirements	482
<b>Making Sense of Laws for Information Security Compliance</b>	<b>486</b>
<b>CHAPTER SUMMARY</b>	<b>487</b>
<b>KEY CONCEPTS AND TERMS</b>	<b>488</b>
<b>CHAPTER 15 ASSESSMENT</b>	<b>488</b>
<b>ENDNOTES</b>	<b>489</b>

<b>APPENDIX A</b>	<b>Answer Key</b>	<b>491</b>
<b>APPENDIX B</b>	<b>Standard Acronyms</b>	<b>493</b>
<b>APPENDIX C</b>	<b>Earning the CompTIA Security+ Certification</b>	<b>495</b>
	<b>Glossary of Key Terms</b>	<b>498</b>
	<b>References</b>	<b>522</b>
	<b>Index</b>	<b>527</b>

# Preface

## Purpose of This Book

This book is part of the Information Systems Security & Assurance (ISSA) Series from Jones & Bartlett Learning ([www.issaseries.com](http://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, 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 forward-thinking—putting you in the position to solve the cybersecurity challenges not just of today, but of tomorrow, as well.

Part I of this book 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 book 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.

## **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 both to clarify the material and to 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 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 majors or information science majors, students at a 2-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

This is the flagship book of the Information Systems Security & Assurance (ISSA) Series from Jones & Bartlett Learning ([www.issaseries.com](http://www.issaseries.com)). The ISSA series was designed for IT security and information assurance curriculums and courseware for those colleges and universities needing a hands-on approach to delivering an information systems security and information assurance degree program whose graduates would be ready for the work force.

The entire ISSA series was developed by information systems security professionals, consultants, and recognized leaders in the field of information systems security, all of whom contributed to each word, sentence, paragraph, and chapter. The dedication and perseverance displayed by those involved was driven by a single passion and a common goal: “to help educate today’s information systems security practitioner” by creating the most up-to-date textbooks, courseware, and hands-on labs to ensure job and skill-set readiness for information systems security practitioners.

Thank you to Jones & Bartlett Learning for having the vision and patience to champion this effort and build the world’s best information systems security content and curriculum. Thank you to Michael Solomon and Jeff Parker and the entire Jones & Bartlett Learning team who contributed to this book and entire ISSA Series during the past 6 months of development.

And last but not least, I would like to thank my wife, MiYoung Kim, who is and always will be by my side. I love you more each day.

*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. And thanks so much to Stacey and Noah for your help in researching the many diverse topics.

*Michael G. Solomon*

# The Authors

**David Kim** is the president of Security Evolutions, Inc. (SEI; [www.security-evolutions.com](http://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 healthcare 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**, CISSP, PMP, CISM, is a full-time security and OpenEdge speaker, consultant, author, and gamification evangelist who specializes in leading teams in achieving and maintaining secure IT environments. As an IT professional and consultant since 1987, he has led projects for many major organizations and has authored and contributed to numerous books and training courses. From 1998 until 2001, he was an instructor in the Kennesaw State University's Computer Science and Information Sciences (CSIS) department, and currently teaches graduate Computer Science and Security courses at the University of the Cumberlands. Michael is also a PhD candidate in Computer Science and Informatics at Emory University.

# **PART I**

---

## **The Need for Information Security**

**CHAPTER 1** Information Systems Security **2**

**CHAPTER 2** The Internet of Things is Changing  
How We Live **47**

**CHAPTER 3** Malicious Attacks, Threats,  
and Vulnerabilities **72**

**CHAPTER 4** The Drivers of the Information  
Security Business **112**



# Information Systems Security

**T**HE INTERNET HAS CHANGED DRAMATICALLY from its origins. It has grown from a tool used by a small number of universities and government agencies to a worldwide network with more than 3 billion users. As it has grown, it has changed the way people communicate and do business, bringing many opportunities and benefits. Today the Internet continues to grow and expand in new and varied ways. It supports innovation and new services such as IP mobility and smartphone connectivity. When the Internet started, the majority of connected devices were solely computers, whether for personal use or within a company. In the most recent years, however, an increasing variety of devices beyond computers, including smartphones, smart cars, appliances, vending machines, smart homes, and smart buildings, can connect and share data.

The Internet as we know it today is expanding rapidly as the **Internet of Things (IoT)** takes over and impacts our day-to-day lives. Although the Internet officially started back in 1969, the extent to which people depend on the Internet is new. Today, people interact with the Internet and cyberspace as part of normal day-to-day living. This includes personal use and business use. Users must now address issues of privacy data security and business data security. Security threats can come from either personal or business use of your Internet-connected device. Intelligent and aggressive cybercriminals, terrorists, and scam artists lurk in the shadows. Connecting your computers or devices to the Internet immediately exposes them to attack. These attacks result in frustration and hardship. Anyone whose personal information has been stolen (called **identity theft**) can attest to that. Worse, attacks on computers and networked devices are a threat to the national economy, which depends on **e-commerce**. Even more important, cyberattacks threaten national security. For example, terrorist attackers could shut down electricity grids and disrupt military communication.

You can make a difference. The world needs people who understand computer security and who can protect computers and networks from criminals and terrorists. Remember, it's all about securing your sensitive data. If you have sensitive data, you must protect it. To get you started, this chapter gives an overview of information systems security concepts and terms that you must understand to stop cyberattacks.

## Chapter 1 Topics

---

This chapter covers the following topics and concepts:

- What unauthorized access and data breaches are
- What information systems security is
- What the tenets of information systems security are
- What the seven domains of an IT infrastructure are
- What the weakest link in an IT infrastructure is
- How an IT security policy framework can reduce risk
- How a data classification standard affects an IT infrastructure's security needs

## Chapter 1 Goals

---

When you complete this chapter, you will be able to:

- Describe how unauthorized access can lead to a data breach
- Relate how availability, integrity, and confidentiality requirements affect the seven domains of a typical IT infrastructure
- Describe the risk, threats, and vulnerabilities commonly found within the seven domains
- Identify a layered security approach throughout the seven domains
- Develop an IT security policy framework to help reduce risk from common threats and vulnerabilities
- Relate how a data classification standard affects the seven domains

## Information Systems Security

---

Today's **Internet** is a worldwide network with more than 2 billion users. It includes almost every government, business, and organization on Earth. However, having that many users on the same network wouldn't solely have been enough to make the Internet a game-changing innovation. These users needed some type of mechanism to link documents and resources across computers. In other words, a user on computer A needed an easy way to open a document on computer B. This need gave rise to a system that defines how documents and resources are related across network machines. The name of this system is the **World Wide Web (WWW)**. You may know it as **cyberspace** or simply as the Web. Think of it this way: The Internet links communication networks to one another. The Web is the connection of websites, webpages, and digital content on those networked computers. Cyberspace is all the accessible users, networks, webpages, and applications working in this worldwide electronic realm.

### Recent Data Breaches in the United States (2013–2015)

The past couple of years have seen a dramatic increase in the number of reported **data breaches** in the United States. Both the public sector and the private sector have fallen victim. **TABLE 1-1** lists a summary of recent data breaches, the affected organization, and the impact of the data breach to that organization.

**TABLE 1-1** Recent data breaches in the United States, 2013–2015.

ORGANIZATION	DATA BREACH	IMPACT OF DATA BREACH
Adobe Systems Incorporated: Software subscription database	In a breach on October 3, 2013, Adobe announced that hackers had published data for 150 million accounts and had stolen encrypted customer credit card data. Logon credentials were also compromised for an undetermined number of Adobe user accounts.	The hackers stole 3 million credit card records and accessed 160,000 Social Security numbers (SSNs). Adobe has offered a year's worth of credit monitoring to customers affected by the breach.
Anthem, Inc.: Blue Cross Blue Shield customer database	<p>On February 4, 2015, Anthem disclosed that criminal hackers had broken into its servers and potentially stolen from its servers over 37.5 million records that contain personally identifiable information.</p> <p>On February 24, 2015, Anthem raised the number of victims to 78.8 million people whose personal information was affected. The data breach extended into multiple brands Anthem uses to market its health care plans, including Anthem Blue Cross, Anthem Blue Cross and Blue Shield, Blue Cross and Blue Shield of Georgia, Empire Blue Cross and BlueShield, Amerigroup, Caremore, and UniCare.</p>	<p>Individuals whose data was stolen could have problems resulting from identity theft for the rest of their lives.</p> <p>Anthem had a \$100 million insurance policy covering cyberattacks from American International Group One.</p>

**ORGANIZATION**

Excellus BlueCross  
BlueShield: Blue Cross Blue  
Shield customer database

**DATA BREACH**

Personal data from more than 10 million members became exposed after the company's IT systems were breached, beginning as far back as December 2013. Among the affected individuals in the Excellus breach are members of other Blue Cross Blue Shield plans who sought treatment in the 31-county upstate New York service area of Excellus, according to the company. Compromised data includes names, addresses, birthdates, SSNs, health plan ID numbers, and financial account information, as well as claims data and clinical information.

**IMPACT OF DATA BREACH**

The suit against Excellus alleges that the health insurer failed to fulfill its legal duty to protect the sensitive information of its customers and those customers whose data were stored in its systems. In addition, the suit alleges that Excellus knew about the security breach for over one month before it publicly disclosed the incident.

Hilton Hotels & Resorts:  
Travel industry customer  
and credit card database

After multiple banks suspected a credit card breach at Hilton properties across the country, Hilton acknowledged an intrusion involving malicious software had been found on some point-of-sale systems. Hilton said the stolen data included cardholder names, payment card numbers, security codes, and expiration dates, but no addresses or personal identification numbers.

Hilton identified and took action to eradicate unauthorized malware that targeted payment card information and strengthened its security. The company offered one year of free credit monitoring to affected customers.

Target Corp.: Customer and  
credit card database of the  
nationwide retailer

In December 2013, a data breach of Target's systems affected up to 110 million customers. Compromised customer information included names, phone numbers, email, and mailing addresses.

Target agreed to reimburse some costs that financial institutions incurred as a result of the breach, but the retailer has failed to reach a settlement with MasterCard over the resulting dispute.

(continues)

**TABLE 1-1** Recent data breaches in the United States, 2013–2015. (*Continued*)

<b>ORGANIZATION</b>	<b>DATA BREACH</b>	<b>IMPACT OF DATA BREACH</b>
Experian Information Solutions, Inc., and T-Mobile USA, Inc.: Database of T-Mobile customers applying for credit	On September 15, 2015, Experian discovered that attackers had breached one North American business unit server containing the personal data of about 15 million T-Mobile customers who had applied for credit. T-Mobile shared this information with Experian to process credit checks or provide financing. Social Security and credit card information was compromised. The Internal Revenue Service (IRS) has confirmed that 13,673 U.S. citizens have been victimized through the filing of \$65 million in fraudulent individual income tax returns as a result of this data breach.	T-Mobile is suffering reputational and financial damage because of the actions of a third-party partner and not its own, notwithstanding the carrier's choice of business partners.
Sony Pictures Entertainment: Confidential files, emails, and employee data	On November 24, 2014, a hacker group identifying itself with the name Guardians of Peace leaked confidential data from the Sony Pictures film studio. The data leak included personal information about Sony Pictures employees and their families, emails between employees, information about Sony executive salaries, copies of then-unreleased Sony films, and other information. In December, the FBI identified the Guardians of Peace as acting on behalf of the North Korean government.	On January 2, 2015, U.S. President Barack Obama issued an executive order enacting additional sanctions against the North Korean government and a North Korean arms dealer, specifically citing this cyberattack and ongoing North Korean policies. Obama also issued a legislative proposal to Congress to update current laws to better respond to cybercrimes like the Sony hack and to be able to prosecute such crimes compatibly with similar offline crimes while protecting citizens' privacy.

**ORGANIZATION**

U.S. Office of Personnel Management : Agency of the U.S. Federal government

**DATA BREACH**

In June 2015, the U.S. Office of Personnel Management (OPM) announced that it had been the target of a data breach impacting approximately 22 million people.

The data breach was noticed by the OPM in April 2015. Federal officials described it as among the largest breaches of government data in the history of the United States. Information targeted in the breach included personally identifiable information such as SSNs as well as names, dates, and places of birth and addresses. The hack went deeper than initially believed and likely involved theft of detailed security clearance-related background information.

**IMPACT OF DATA BREACH**

The data breach has created a massive counterintelligence threat that could easily last 40 years. For every nonmarried federal employee in the background investigation database, at least four out of five people will require monitoring.

For those who have been married or married more than once, the number of affected people is at least 12 out of 14.

The Wendy's Co.: Customer and credit card database of the nationwide fast-food retailer

After becoming suspicious in December 2015, the Ohio-based burger chain began looking into reports of unusual activity on credit cards used at Wendy's locations across the country. The company hired a team of cybersecurity experts to help assess the damage and is cooperating with law enforcement in a criminal investigation. Customers at as many as 6,000 Wendy's locations may have been affected.

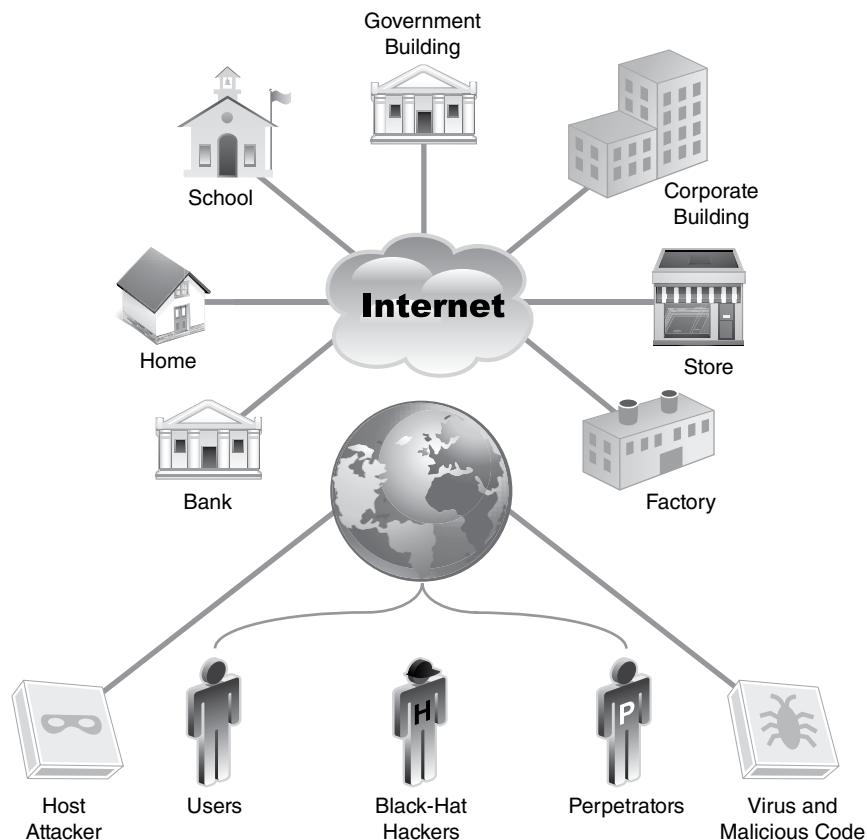
The investigation is new and ongoing, but card breaches are becoming more and more common in the restaurant industry.

Restaurant chains are especially susceptible, likely because of their use of outdated technology.

Unfortunately, when you connect to cyberspace, you also open the door to a lot of bad guys. They want to find you and steal your data. Every computer or device that connects to the Internet is at risk, creating an Internet of Things (IoT) that supports users in all aspects of their lives. Like outer space, the maturing Internet is a new frontier. There is no Internet government or central authority. It is full of challenges—and questionable behavior. This questionable behavior is evident given the data breaches we've seen in the past three years alone. In the United States, public and private sectors have been compromised through unauthorized access and data breach attacks. These recent attacks have been committed by individuals, organized cybercriminals, and attackers from other nations. The quantity of cyberattacks on U.S. interests is increasing.

With the Internet of Things (IoT) now connecting personal devices, home devices, and vehicles to the Internet, there are even more data to steal. All users must defend their information from attackers. **Cybersecurity** is the duty of every government that wants to ensure its national security. Data security is the responsibility of every organization that needs to protect its information assets and sensitive data (e.g., SSNs, credit card numbers, and the like). And it's the job of all of us to protect our own data. **FIGURE 1-1** illustrates this new frontier.

The components that make up cyberspace are not automatically secure. These components include cabling, physical networks, operating systems, and software applications that computers use to connect to the Internet. At the heart of the problem is the lack of security in the **Transmission Control Protocol/Internet Protocol (TCP/IP)** communications protocol. This protocol



**FIGURE 1-1**

Cyberspace: the new frontier.

is the language that computers most commonly use to communicate across the Internet. (A **protocol** is a list of rules and methods for communicating.) TCP/IP is not just one protocol but a suite of protocols developed for communicating across a network. Named after the two most important protocols, TCP/IP works together to allow any two computers to communicate. Connecting two or more computers creates a network. TCP/IP breaks messages into chunks, or packets, to send data between networked computers. The problem lies in the fact that data are readable within each IP packet using simple software available to anyone. This readable mode is known as **cleartext**. That means you must hide or encrypt the data sent inside a TCP/IP packet to make the data more secure. **FIGURE 1-2** shows the data within the TCP/IP packet structure.

All this raises the question: If the Internet is so unsafe, why did everyone connect to it so readily? The answer is the huge growth of the Web from the mid-1990s to the early 2000s. Connecting to the Internet gave anyone instant access to the Web and its many resources. The appeal of easy worldwide connectivity drove the demand to connect. This demand and subsequent growth helped drive costs lower for high-speed communications. Households, businesses, and governments gained affordable high-speed Internet access. And as wireless and cellular connections have become more common and affordable, it has become easier to

**FIGURE 1-2**

TCP/IP communications are in cleartext.

