Transition Guide

By David Kim • Michael G. Solomon
Paperback
575 Pages • ©2018

Main Updates

- Maps fully to the six major domains of the CompTIA Security+ SYO-401 Certification exam
- Updated to include coverage on recent compliance law and standards updates, including FISMA, NIST SP800-171, and PCI DSS v3.2
- New content on advanced malware and APT attacks to the end points such as ransomware and crypto locker
- Addresses data breach and data breach incident response planning
- Introduces recent "Internet of Things" risk threats and privacy issues
- Available with the Virtual Security Cloud Labs which provide a hands-on, immersive mock IT infrastructure enabling students to test their skills with realistic security scenarios

Major Chapter Changes Are Listed Below

Chapter 1:
- Introduction of the Internet of Things (IoT)
- Updates to recent data breaches
- Emphasis on data breach prevention

Chapter 2:
- New chapter on the IoT
- Impact that security, compliance and privacy has on the IoT
• Convergence of business and personal communications and data

Chapter 3:
• Updated content on malware and malicious software
• Recent case studies of malware attacks, including ransomware
• Next generation advanced persistent threats (APT)

Chapter 4:
• Updates to compliance law content
• New content on mobility and bring your own device (BYOD)
• New content on endpoint and device security

Chapter 5:
• Updated to reflect the latest access control strategies for today’s operating systems
• More extensive coverage of biometrics and the latest technology used in access control

Chapter 6:
• Includes discussion of how data and process outsourcing affects security operations
• More emphasis on the importance of including security early in the software development process

Chapter 7:
• Updated references and content to reflect the latest compliance requirements
• Expands the emphasis on assessing security controls for compliance

Chapter 8:
• Moved risk management definitions and topics into a single chapter
• Updated content and examples address recovery issues today’s IT organizations face, including cloud components

Chapter 9:
• Updated content includes the latest trends in cryptography from academia and industry
• Expands discussions of cryptography basics and implementation

Chapter 10:
• Expanded content covers the latest network protocol and practical uses
• Includes the latest wireless network and network device advances

Chapter 11:
• More focus on the latest malware types, including ransomware
• Includes more details on the most common malware attacks

Chapter 12
• Updated content includes the latest information security standards

Chapter 13:
• Updates to education, training, and certification programs in Information Systems Security
• Upgrades to undergraduate and graduate degree programs in Cybersecurity and Information Assurance

Chapter 14:
• Updates to US Federal Government Department of Defense standards for education and training
• Updates to numerous professional certification programs

Chapter 15
• Updates to US based compliance laws
• New content on FISMA 2014
• New content on PCI DSS v3.2

Table of Contents Comparison: Outlines Chapter Reorganization

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Part 1 The Need for Information Security</td>
<td>Part 1 The Need for Information Security</td>
</tr>
<tr>
<td>Chapter 1 Information Systems Security</td>
<td>Chapter 1 Information Systems Security</td>
</tr>
<tr>
<td>Chapter 2 Changing the Way People and Businesses do Business</td>
<td>Chapter 2 The Internet of Things is Changing How We Live</td>
</tr>
<tr>
<td>Chapter 3 Malicious Attacks, Threats, and Vulnerabilities</td>
<td>Chapter 3 Malicious Attacks, Threats, and Vulnerabilities</td>
</tr>
<tr>
<td>Chapter 4 The Drivers of Information Security Business</td>
<td>Chapter 4 The Drivers of the Information Security Business</td>
</tr>
<tr>
<td>Part 2 The Systems Security Certified Practitioner (SSCP) Professional Certification from (ISC)²</td>
<td>Part 2 Securing Today's Information Systems</td>
</tr>
<tr>
<td>Chapter 5 Access Controls</td>
<td>Chapter 5 Access Controls</td>
</tr>
<tr>
<td>Chapter 6 Security Operations and Administration</td>
<td>Chapter 6 Security Operations and Administration</td>
</tr>
<tr>
<td>Chapter 7 Auditing, Testing, and Monitoring</td>
<td>Chapter 7 Auditing, Testing, and Monitoring</td>
</tr>
<tr>
<td>Chapter 8 Risk, Response, and Recovery</td>
<td>Chapter 8 Risk, Response, and Recovery</td>
</tr>
<tr>
<td>Chapter 9 Cryptography</td>
<td>Chapter 9 Cryptography</td>
</tr>
<tr>
<td>Chapter 10 Networks and Communications</td>
<td>Chapter 10 Networks and Telecommunications</td>
</tr>
<tr>
<td>Chapter 11 Malicious Code and Activity</td>
<td>Chapter 11 Malicious Code and Activity</td>
</tr>
<tr>
<td>Chapter 12 Information Security Standards</td>
<td>Chapter 12 Information Security Standards</td>
</tr>
<tr>
<td>Chapter 13 Information Security Education and Training</td>
<td>Chapter 13 Information Systems Security Education and Training</td>
</tr>
<tr>
<td>Chapter 14 Information Security Professional Certifications</td>
<td>Chapter 14 Information Security Professional Certifications</td>
</tr>
<tr>
<td>Chapter 15 US Compliance Laws</td>
<td>Chapter 15 U.S. Compliance Laws</td>
</tr>
</tbody>
</table>