

# CISSP®

## Certified Information Systems Security Professional Study Guide Seventh Edition



James Michael Stewart

Mike Chapple

Darril Gibson

 **SYBEX®**  
A Wiley Brand

# Acknowledgments

I'd like to express my thanks to Sybex for continuing to support this project. Thanks to Mike Chapple and Darril Gibson for continuing to contribute to this project. Thanks also to all my CISSP course students who have provided their insight and input to improve my training courseware and ultimately this tome. Extra thanks to the seventh edition developmental editor, Alexa Murphy, and technical editor, David Seidl, who performed amazing feats in guiding us to improve this book. Thanks as well to my agent, Carole Jelen, for continuing to assist in nailing down these projects.

To my adoring wife, Cathy: Building a life and a family together has been more wonderful than I could have ever imagined. To Slayde and Remi: You are growing up so fast and learning at an outstanding pace, and you continue to delight and impress me daily. You are both growing into amazing individuals. To my mom, Johnnie: It is wonderful to have you close by. To Mark: No matter how much time has passed or how little we see each other, I have been and always will be your friend. And finally, as always, to Elvis: You were way ahead of the current bacon obsession, with your peanut butter-banana-bacon sandwich; I think that's proof you traveled through time!

—*James Michael Stewart*

Special thanks go to the information security team at the University of Notre Dame, who provided hours of interesting conversation and debate on security issues that inspired and informed much of the material in this book.

I would like to thank the team at Wiley who provided invaluable assistance throughout the book development process. I also owe a debt of gratitude to my literary agent, Carole Jelen of Waterside Productions. My coauthors, James Michael Stewart and Darril Gibson, were great collaborators. David Seidl, our diligent and knowledgeable technical editor, provided valuable insight as we brought this edition to press.

I'd also like to thank the many people who participated in the production of this book but whom I never had the chance to meet: the graphics team, the production staff, and all of those involved in bringing this book to press.

—*Mike Chapple*

Thanks to Carol Long and Carole Jelen for helping get this update in place before (ISC)<sup>2</sup> released the objectives. This helped us get a head start on this new edition and we appreciate your efforts. It's been a pleasure working with talented people like James Michael Stewart and Mike Chapple. Thanks to both of you for all your work and collaborative efforts on this project. The technical editor, Dave Seidl, provided us with some outstanding feedback and this book is better because of his efforts. Thanks again, David. Last, thanks to the team at Sybex (including project managers, editors, and graphics artists) for all the work you did helping us get this book to print.

—*Darril Gibson*

# About the Authors

**James Michael Stewart**, CISSP, has been writing and training for more than 20 years, with a current focus on security. He has been teaching CISSP training courses since 2002, not to mention other courses on Internet security and ethical hacking/penetration testing. He is the author of and contributor to more than 75 books and numerous courseware sets on security certification, Microsoft topics, and network administration. More information about Michael can be found at his website: [www.impactonline.com](http://www.impactonline.com).

**Mike Chapple**, CISSP, Ph.D., is Senior Director for IT Service Delivery at the University of Notre Dame. In the past, he was chief information officer of Brand Institute and an information security researcher with the National Security Agency and the U.S. Air Force. His primary areas of expertise include network intrusion detection and access controls. Mike is a frequent contributor to TechTarget's SearchSecurity site and the author of more than 25 books including *CompTIA Security+ Training Kit* and *Information Security Illuminated*. Mike can be found on Twitter @mchapple.

**Darril Gibson**, CISSP, is the CEO of YCDA, LLC (short for You Can Do Anything) and he has authored or coauthored more than 35 books. Darril regularly writes, consults, and teaches on a wide variety of technical and security topics and holds several certifications. He regularly posts blog articles at <http://blogs.getcertifiedgetahead.com/> about certification topics and uses that site to help people stay abreast of changes in certification exams. He loves hearing from readers, especially when they pass an exam after using one of his books, and you can contact him through the blogging site.

# Contents at a Glance

<i>Introduction</i>		<i>xxxiii</i>
<i>Assessment Test</i>		<i>xlii</i>
<b>Chapter 1</b>	Security Governance Through Principles and Policies	1
<b>Chapter 2</b>	Personnel Security and Risk Management Concepts	47
<b>Chapter 3</b>	Business Continuity Planning	93
<b>Chapter 4</b>	Laws, Regulations, and Compliance	123
<b>Chapter 5</b>	Protecting Security of Assets	157
<b>Chapter 6</b>	Cryptography and Symmetric Key Algorithms	189
<b>Chapter 7</b>	PKI and Cryptographic Applications	231
<b>Chapter 8</b>	Principles of Security Models, Design, and Capabilities	269
<b>Chapter 9</b>	Security Vulnerabilities, Threats, and Countermeasures	313
<b>Chapter 10</b>	Physical Security Requirements	385
<b>Chapter 11</b>	Secure Network Architecture and Securing Network Components	425
<b>Chapter 12</b>	Secure Communications and Network Attacks	499
<b>Chapter 13</b>	Managing Identity and Authentication	555
<b>Chapter 14</b>	Controlling and Monitoring Access	593
<b>Chapter 15</b>	Security Assessment and Testing	629
<b>Chapter 16</b>	Managing Security Operations	659
<b>Chapter 17</b>	Preventing and Responding to Incidents	697
<b>Chapter 18</b>	Disaster Recovery Planning	759
<b>Chapter 19</b>	Incidents and Ethics	803
<b>Chapter 20</b>	Software Development Security	837
<b>Chapter 21</b>	Malicious Code and Application Attacks	881
<b>Appendix A</b>	Answers to Review Questions	915
<b>Appendix B</b>	Answers to Written Labs	953
<b>Appendix C</b>	About the Additional Study Tools	967
<b>Index</b>		<b>971</b>

# Contents

<i>Introduction</i>	<i>xxxiii</i>	
<i>Assessment Test</i>	<i>xlii</i>	
<b>Chapter 1</b>	<b>Security Governance Through Principles and Policies</b>	<b>1</b>
Understand and Apply Concepts of Confidentiality, Integrity, and Availability		3
Confidentiality		4
Integrity		5
Availability		6
Other Security Concepts		8
Protection Mechanisms		12
Layering		12
Abstraction		12
Data Hiding		13
Encryption		13
Apply Security Governance Principles		13
Alignment of Security Function to Strategy, Goals, Mission, and Objectives		14
Organizational Processes		16
Security Roles and Responsibilities		22
Control Frameworks		23
Due Care and Due Diligence		24
Develop and Implement Documented Security Policy, Standards, Procedures, and Guidelines		25
Security Policies		25
Security Standards, Baselines, and Guidelines		26
Security Procedures		27
Understand and Apply Threat Modeling		28
Identifying Threats		30
Determining and Diagramming Potential Attacks		32
Performing Reduction Analysis		33
Prioritization and Response		34
Integrate Security Risk Considerations into Acquisition Strategy and Practice		35
Summary		36
Exam Essentials		38
Written Lab		41
Review Questions		42

<b>Chapter 2</b>	<b>Personnel Security and Risk Management Concepts</b>	<b>47</b>
	Contribute to Personnel Security Policies	49
	Employment Candidate Screening	52
	Employment Agreements and Policies	53
	Employment Termination Processes	54
	Vendor, Consultant, and Contractor Controls	56
	Compliance	57
	Privacy	57
	Security Governance	59
	Understand and Apply Risk Management Concepts	60
	Risk Terminology	61
	Identify Threats and Vulnerabilities	63
	Risk Assessment/Analysis	64
	Risk Assignment/Acceptance	72
	Countermeasure Selection and Assessment	73
	Implementation	74
	Types of Controls	75
	Monitoring and Measurement	76
	Asset Valuation	77
	Continuous Improvement	78
	Risk Frameworks	78
	Establish and Manage Information Security Education, Training, and Awareness	81
	Manage the Security Function	82
	Summary	83
	Exam Essentials	84
	Written Lab	88
	Review Questions	89
<b>Chapter 3</b>	<b>Business Continuity Planning</b>	<b>93</b>
	Planning for Business Continuity	94
	Project Scope and Planning	95
	Business Organization Analysis	96
	BCP Team Selection	96
	Resource Requirements	98
	Legal and Regulatory Requirements	100
	Business Impact Assessment	101
	Identify Priorities	101
	Risk Identification	102
	Likelihood Assessment	104
	Impact Assessment	104
	Resource Prioritization	106
	Continuity Planning	107
	Strategy Development	107

	Provisions and Processes	108
	Plan Approval	109
	Plan Implementation	110
	Training and Education	110
	BCP Documentation	110
	Continuity Planning Goals	111
	Statement of Importance	111
	Statement of Priorities	111
	Statement of Organizational Responsibility	111
	Statement of Urgency and Timing	112
	Risk Assessment	112
	Risk Acceptance/Mitigation	112
	Vital Records Program	113
	Emergency-Response Guidelines	113
	Maintenance	114
	Testing and Exercises	114
	Summary	114
	Exam Essentials	115
	Written Lab	117
	Review Questions	118
<b>Chapter 4</b>	<b>Laws, Regulations, and Compliance</b>	<b>123</b>
	Categories of Laws	124
	Criminal Law	124
	Civil Law	126
	Administrative Law	126
	Laws	127
	Computer Crime	127
	Intellectual Property	132
	Licensing	138
	Import/Export	139
	Privacy	139
	Compliance	146
	Contracting and Procurement	147
	Summary	148
	Exam Essentials	149
	Written Lab	151
	Review Questions	152
<b>Chapter 5</b>	<b>Protecting Security of Assets</b>	<b>157</b>
	Classifying and Labeling Assets	158
	Defining Sensitive Data	158
	Defining Classifications	160
	Defining Data Security Requirements	163

Understanding Data States	164
Managing Sensitive Data	165
Protecting Confidentiality with Cryptography	172
Identifying Data Roles	174
Data Owners	174
System Owners	175
Business/Mission Owners	176
Data Processors	176
Administrators	177
Custodians	178
Users	178
Protecting Privacy	178
Using Security Baselines	179
Scoping and Tailoring	180
Selecting Standards	180
Summary	181
Exam Essentials	182
Written Lab	183
Review Questions	184
<b>Chapter 6</b>	<b>Cryptography and Symmetric Key Algorithms</b>
	<b>189</b>
Historical Milestones in Cryptography	190
Caesar Cipher	190
American Civil War	191
Ultra vs. Enigma	192
Cryptographic Basics	192
Goals of Cryptography	192
Cryptography Concepts	194
Cryptographic Mathematics	196
Ciphers	201
Modern Cryptography	208
Cryptographic Keys	208
Symmetric Key Algorithms	209
Asymmetric Key Algorithms	210
Hashing Algorithms	213
Symmetric Cryptography	214
Data Encryption Standard	214
Triple DES	216
International Data Encryption Algorithm	217
Blowfish	217
Skipjack	217
Advanced Encryption Standard	218
Symmetric Key Management	219
Cryptographic Life Cycle	222



	Summary	222
	Exam Essentials	223
	Written Lab	225
	Review Questions	226
<b>Chapter 7</b>	<b>PKI and Cryptographic Applications</b>	<b>231</b>
	Asymmetric Cryptography	232
	Public and Private Keys	232
	RSA	233
	El Gamal	235
	Elliptic Curve	235
	Hash Functions	236
	SHA	237
	MD2	238
	MD4	238
	MD5	239
	Digital Signatures	240
	HMAC	241
	Digital Signature Standard	242
	Public Key Infrastructure	242
	Certificates	243
	Certificate Authorities	243
	Certificate Generation and Destruction	245
	Asymmetric Key Management	246
	Applied Cryptography	247
	Portable Devices	247
	Email	248
	Web Applications	249
	Digital Rights Management	252
	Networking	255
	Cryptographic Attacks	258
	Summary	261
	Exam Essentials	261
	Written Lab	264
	Review Questions	265
<b>Chapter 8</b>	<b>Principles of Security Models, Design, and Capabilities</b>	<b>269</b>
	Implement and Manage Engineering Processes Using	
	Secure Design Principles	270
	Objects and Subjects	271
	Closed and Open Systems	271
	Techniques for Ensuring Confidentiality, Integrity, and Availability	272

Controls	274
Trust and Assurance	274
Understand the Fundamental Concepts of Security Models	275
Trusted Computing Base	276
State Machine Model	278
Information Flow Model	279
Noninterference Model	279
Take-Grant Model	280
Access Control Matrix	280
Bell-LaPadula Model	282
Biba Model	284
Clark-Wilson Model	286
Brewer and Nash Model (aka Chinese Wall)	287
Goguen-Meseguer Model	288
Sutherland Model	288
Graham-Denning Model	288
Select Controls and Countermeasures Based on Systems	
Security Evaluation Models	289
Rainbow Series	290
ITSEC Classes and Required Assurance and Functionality	295
Common Criteria	296
Industry and International Security Implementation Guidelines	299
Certification and Accreditation	300
Understand Security Capabilities of Information Systems	303
Memory Protection	303
Virtualization	303
Trusted Platform Module	303
Interfaces	304
Fault Tolerance	304
Summary	305
Exam Essentials	305
Written Lab	307
Review Questions	308
<b>Chapter 9</b>	
<b>Security Vulnerabilities, Threats, and Countermeasures</b>	<b>313</b>
Assess and Mitigate Security Vulnerabilities	314
Hardware	315
Input/Output Structures	335
Firmware	336

Client-Based	337
Applets	337
Local Caches	339
Server Based	341
Database Security	341
Aggregation	341
Inference	342
Data Mining and Data Warehousing	342
Data Analytics	343
Large-Scale Parallel Data Systems	344
Distributed Systems	344
Cloud Computing	346
Grid Computing	347
Peer to Peer	348
Industrial Control Systems	348
Assess and Mitigate Vulnerabilities in Web-Based Systems	349
Assess and Mitigate Vulnerabilities in Mobile Systems	350
Device Security	352
Application Security	355
BYOD Concerns	357
Assess and Mitigate Vulnerabilities in Embedded Devices and Cyber-Physical Systems	360
Examples of Embedded and Static Systems	360
Methods of Securing	362
Essential Security Protection Mechanisms	364
Technical Mechanisms	364
Security Policy and Computer Architecture	367
Policy Mechanisms	367
Common Architecture Flaws and Security Issues	369
Covert Channels	369
Attacks Based on Design or Coding Flaws and Security Issues	370
Programming	373
Timing, State Changes, and Communication Disconnects	373
Technology and Process Integration	374
Electromagnetic Radiation	374
Summary	375
Exam Essentials	376
Written Lab	379
Review Questions	380

<b>Chapter 10</b>	<b>Physical Security Requirements</b>	<b>385</b>
	Apply Secure Principles to Site and Facility Design	386
	Secure Facility Plan	387
	Site Selection	387
	Visibility	388
	Natural Disasters	388
	Facility Design	388
	Design and Implement Physical Security	389
	Equipment Failure	390
	Wiring Closets	391
	Server Rooms	393
	Media Storage Facilities	394
	Evidence Storage	395
	Restricted and Work Area Security (e.g., Operations Centers)	395
	Datacenter Security	396
	Utilities and HVAC Considerations	399
	Water Issues (e.g., Leakage, Flooding)	402
	Fire Prevention, Detection, and Suppression	402
	Implement and Manage Physical Security	407
	Perimeter (e.g., Access Control and Monitoring)	407
	Internal Security (e.g., Escort Requirements/Visitor Control, Keys, and Locks)	409
	Summary	415
	Exam Essentials	416
	Written Lab	420
	Review Questions	421
<b>Chapter 11</b>	<b>Secure Network Architecture and Securing Network Components</b>	<b>425</b>
	OSI Model	426
	History of the OSI Model	427
	OSI Functionality	427
	Encapsulation/Deencapsulation	428
	OSI Layers	429
	TCP/IP Model	437
	TCP/IP Protocol Suite Overview	438
	Converged Protocols	452
	Content Distribution Networks	453
	Wireless Networks	454
	Securing Wireless Access Points	454
	Securing the SSID	456
	Conducting a Site Survey	457

Using Secure Encryption Protocols	458
Determining Antenna Placement	461
Antenna Types	461
Adjusting Power Level Controls	461
Using Captive Portals	462
General Wi-Fi Security Procedure	462
Secure Network Components	463
Network Access Control	464
Firewalls	465
Endpoint Security	469
Other Network Devices	469
Cabling, Wireless, Topology, and Communications	
Technology	473
Network Cabling	473
Network Topologies	477
Wireless Communications and Security	480
LAN Technologies	485
Summary	490
Exam Essentials	490
Written Lab	494
Review Questions	495
<b>Chapter 12</b>	<b>Secure Communications and Network Attacks</b>
	<b>499</b>
Network and Protocol Security Mechanisms	500
Secure Communications Protocols	501
Authentication Protocols	502
Secure Voice Communications	503
Voice over Internet Protocol (VoIP)	503
Social Engineering	504
Fraud and Abuse	505
Multimedia Collaboration	507
Remote Meeting	508
Instant Messaging	508
Manage Email Security	508
Email Security Goals	509
Understand Email Security Issues	510
Email Security Solutions	511
Remote Access Security Management	513
Plan Remote Access Security	515
Dial-Up Protocols	516
Centralized Remote Authentication Services	517
Virtual Private Network	517
Tunneling	518
How VPNs Work	519

Common VPN Protocols	520
Virtual LAN	522
Virtualization	523
Virtual Software	523
Virtual Networking	524
Network Address Translation	525
Private IP Addresses	526
Stateful NAT	527
Static and Dynamic NAT	528
Automatic Private IP Addressing	528
Switching Technologies	530
Circuit Switching	530
Packet Switching	531
Virtual Circuits	532
WAN Technologies	532
WAN Connection Technologies	534
Dial-Up Encapsulation Protocols	536
Miscellaneous Security Control Characteristics	537
Transparency	537
Verify Integrity	537
Transmission Mechanisms	538
Security Boundaries	539
Prevent or Mitigate Network Attacks	539
DoS and DDoS	540
Eavesdropping	541
Impersonation/Masquerading	542
Replay Attacks	542
Modification Attacks	542
Address Resolution Protocol Spoofing	542
DNS Poisoning, Spoofing, and Hijacking	543
Hyperlink Spoofing	544
Summary	545
Exam Essentials	546
Written Lab	549
Review Questions	550
<b>Chapter 13</b>	<b>Managing Identity and Authentication</b>
	<b>555</b>
Controlling Access to Assets	556
Comparing Subjects and Objects	557
Types of Access Control	557
The CIA Triad	560
Comparing Identification and Authentication	560
Registration and Proofing of Identity	561
Authorization and Accountability	561

	Authentication Factors	563
	Passwords	564
	Smartcards and Tokens	566
	Biometrics	568
	Multifactor Authentication	572
	Device Authentication	572
	Implementing Identity Management	573
	Single Sign-On	573
	Credential Management Systems	578
	Integrating Identity Services	579
	Managing Sessions	579
	AAA Protocols	580
	Managing the Identity and Access Provisioning Life Cycle	582
	Provisioning	582
	Account Review	583
	Account Revocation	584
	Summary	585
	Exam Essentials	586
	Written Lab	588
	Review Questions	589
<b>Chapter 14</b>	<b>Controlling and Monitoring Access</b>	<b>593</b>
	Comparing Access Control Models	594
	Comparing Permissions, Rights, and Privileges	594
	Understanding Authorization Mechanisms	595
	Defining Requirements with a Security Policy	596
	Implementing Defense in Depth	597
	Discretionary Access Controls	598
	Nondiscretionary Access Controls	598
	Understanding Access Control Attacks	604
	Risk Elements	605
	Identifying Assets	605
	Identifying Threats	607
	Identifying Vulnerabilities	609
	Common Access Control Attacks	610
	Summary of Protection Methods	619
	Summary	621
	Exam Essentials	622
	Written Lab	624
	Review Questions	625
<b>Chapter 15</b>	<b>Security Assessment and Testing</b>	<b>629</b>
	Building a Security Assessment and Testing Program	630
	Security Testing	630

Security Assessments	631
Security Audits	632
Performing Vulnerability Assessments	634
Vulnerability Scans	634
Penetration Testing	642
Testing Your Software	643
Code Review and Testing	644
Interface Testing	646
Misuse Case Testing	648
Test Coverage Analysis	648
Implementing Security Management Processes	649
Log Reviews	649
Account Management	649
Backup Verification	650
Key Performance and Risk Indicators	650
Summary	650
Exam Essentials	651
Written Lab	653
Review Questions	654
<b>Chapter 16</b>	<b>Managing Security Operations</b>
	<b>659</b>
Applying Security Operations Concepts	661
Need to Know and Least Privilege	661
Separation of Duties and Responsibilities	663
Job Rotation	666
Mandatory Vacations	666
Monitor Special Privileges	667
Managing the Information Life Cycle	668
Service Level Agreements	669
Addressing Personnel Safety	670
Provisioning and Managing Resources	670
Managing Hardware and Software Assets	671
Protecting Physical Assets	672
Managing Virtual Assets	672
Managing Cloud-based Assets	673
Media Management	675
Managing Configuration	678
Baselining	678
Using Images for Baselining	678
Managing Change	680
Security Impact Analysis	682
Versioning	683
Configuration Documentation	683



	Managing Patches and Reducing Vulnerabilities	684
	Patch Management	684
	Vulnerability Management	685
	Common Vulnerabilities and Exposures	688
	Summary	688
	Exam Essentials	689
	Written Lab	691
	Review Questions	692
<b>Chapter 17</b>	<b>Preventing and Responding to Incidents</b>	<b>697</b>
	Managing Incident Response	698
	Defining an Incident	698
	Incident Response Steps	699
	Implementing Preventive Measures	704
	Basic Preventive Measures	705
	Understanding Attacks	705
	Intrusion Detection and Prevention Systems	715
	Specific Preventive Measures	721
	Logging, Monitoring, and Auditing	731
	Logging and Monitoring	731
	Egress Monitoring	740
	Auditing to Assess Effectiveness	742
	Security Audits and Reviews	745
	Reporting Audit Results	746
	Summary	748
	Exam Essentials	750
	Written Lab	754
	Review Questions	755
<b>Chapter 18</b>	<b>Disaster Recovery Planning</b>	<b>759</b>
	The Nature of Disaster	760
	Natural Disasters	761
	Man-made Disasters	765
	Understand System Resilience and Fault Tolerance	770
	Protecting Hard Drives	771
	Protecting Servers	772
	Protecting Power Sources	773
	Trusted Recovery	773
	Quality of Service	775
	Recovery Strategy	775
	Business Unit and Functional Priorities	776
	Crisis Management	777
	Emergency Communications	777

Workgroup Recovery	778
Alternate Processing Sites	778
Mutual Assistance Agreements	782
Database Recovery	783
Recovery Plan Development	784
Emergency Response	785
Personnel and Communications	786
Assessment	787
Backups and Offsite Storage	787
Software Escrow Arrangements	790
External Communications	791
Utilities	791
Logistics and Supplies	791
Recovery vs. Restoration	791
Training, Awareness, and Documentation	792
Testing and Maintenance	793
Read-Through Test	793
Structured Walk-Through	794
Simulation Test	794
Parallel Test	794
Full-Interruption Test	794
Maintenance	794
Summary	795
Exam Essentials	795
Written Lab	797
Review Questions	798
<b>Chapter 19</b>	<b>Incidents and Ethics</b>
	<b>803</b>
Investigations	804
Investigation Types	804
Evidence	806
Investigation Process	810
Major Categories of Computer Crime	812
Military and Intelligence Attacks	813
Business Attacks	814
Financial Attacks	814
Terrorist Attacks	815
Grudge Attacks	815
Thrill Attacks	817
Incident Handling	817
Common Types of Incidents	818
Response Teams	820
Incident Response Process	821
Interviewing Individuals	824

	Incident Data Integrity and Retention	825
	Reporting and Documenting Incidents	825
	Ethics	826
	(ISC) <sup>2</sup> Code of Ethics	827
	Ethics and the Internet	828
	Summary	829
	Exam Essentials	830
	Written Lab	832
	Review Questions	833
<b>Chapter 20</b>	<b>Software Development Security</b>	<b>837</b>
	Introducing Systems Development Controls	838
	Software Development	838
	Systems Development Life Cycle	844
	Life Cycle Models	847
	Gantt Charts and PERT	853
	Change and Configuration Management	853
	The DevOps Approach	855
	Application Programming Interfaces	856
	Software Testing	857
	Code Repositories	858
	Service-Level Agreements	859
	Software Acquisition	860
	Establishing Databases and Data Warehousing	860
	Database Management System Architecture	861
	Database Transactions	864
	Security for Multilevel Databases	866
	ODBC	868
	Storing Data and Information	869
	Types of Storage	869
	Storage Threats	870
	Understanding Knowledge-based Systems	870
	Expert Systems	870
	Neural Networks	872
	Decision Support Systems	872
	Security Applications	873
	Summary	873
	Exam Essentials	874
	Written Lab	875
	Review Questions	876
<b>Chapter 21</b>	<b>Malicious Code and Application Attacks</b>	<b>881</b>
	Malicious Code	882
	Sources of Malicious Code	882

Viruses	883
Logic Bombs	889
Trojan Horses	889
Worms	890
Spyware and Adware	893
Countermeasures	893
Password Attacks	895
Password Guessing	895
Dictionary Attacks	896
Social Engineering	897
Countermeasures	898
Application Attacks	899
Buffer Overflows	899
Time of Check to Time of Use	900
Back Doors	900
Escalation of Privilege and Rootkits	900
Web Application Security	901
Cross-Site Scripting (XSS)	901
SQL Injection	902
Reconnaissance Attacks	905
IP Probes	905
Port Scans	906
Vulnerability Scans	906
Dumpster Diving	906
Masquerading Attacks	907
IP Spoofing	907
Session Hijacking	908
Summary	908
Exam Essentials	909
Written Lab	910
Review Questions	911
<b>Appendix A</b>	<b>Answers to Review Questions</b>
	<b>915</b>
Chapter 1: Security Governance Through Principles and Policies	916
Chapter 2: Personnel Security and Risk Management Concepts	917
Chapter 3: Business Continuity Planning	918
Chapter 4: Laws, Regulations, and Compliance	920
Chapter 5: Protecting Security of Assets	922
Chapter 6: Cryptography and Symmetric Key Algorithms	924
Chapter 7: PKI and Cryptographic Applications	926
Chapter 8: Principles of Security Models, Design, and Capabilities	927

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures	929
Chapter 10: Physical Security Requirements	931
Chapter 11: Secure Network Architecture and Securing Network Components	932
Chapter 12: Secure Communications and Network Attacks	933
Chapter 13: Managing Identity and Authentication	935
Chapter 14: Controlling and Monitoring Access	937
Chapter 15: Security Assessment and Testing	939
Chapter 16: Managing Security Operations	940
Chapter 17: Preventing and Responding to Incidents	943
Chapter 18: Disaster Recovery Planning	946
Chapter 19: Incidents and Ethics	948
Chapter 20: Software Development Security	949
Chapter 21: Malicious Code and Application Attacks	950
<b>Appendix B</b>	
<b>Answers to Written Labs</b>	<b>953</b>
Chapter 1: Security Governance Through Principles and Policies	954
Chapter 2: Personnel Security and Risk Management Concepts	954
Chapter 3: Business Continuity Planning	955
Chapter 4: Laws, Regulations, and Compliance	956
Chapter 5: Protecting Security of Assets	956
Chapter 6: Cryptography and Symmetric Key Algorithms	957
Chapter 7: PKI and Cryptographic Applications	958
Chapter 8: Principles of Security Models, Design, and Capabilities	958
Chapter 9: Security Vulnerabilities, Threats, and Countermeasures	959
Chapter 10: Physical Security Requirements	959
Chapter 11: Secure Network Architecture and Securing Network Components	960
Chapter 12: Secure Communications and Network Attacks	960
Chapter 13: Managing Identity and Authentication	961
Chapter 14: Controlling and Monitoring Access	962
Chapter 15: Security Assessment and Testing	962
Chapter 16: Managing Security Operations	963
Chapter 17: Preventing and Responding to Incidents	963
Chapter 18: Disaster Recovery Planning	964
Chapter 19: Incidents and Ethics	965
Chapter 20: Software Development Security	965
Chapter 21: Malicious Code and Application Attacks	966

<b>Appendix C</b>	<b>About the Additional Study Tools</b>	<b>967</b>
	Additional Study Tools	968
	Sybex Test Engine	968
	Electronic Flashcards	968
	PDF of Glossary of Terms	968
	Adobe Reader	968
	System Requirements	969
	Using the Study Tools	969
	Troubleshooting	969
	Customer Care	970
	<i>Index</i>	971