
CONTENTS AT A GLANCE

Chapter 1	Becoming a CISSP	1
Chapter 2	Security Trends	19
Chapter 3	Information Security and Risk Management	53
Chapter 4	Access Control	155
Chapter 5	Security Architecture and Design	279
Chapter 6	Physical and Environmental Security	401
Chapter 7	Telecommunications and Network Security	481
Chapter 8	Cryptography	659
Chapter 9	Business Continuity and Disaster Recovery	769
Chapter 10	Legal, Regulations, Compliance, and Investigations	835
Chapter 11	Application Security	905
Chapter 12	Operations Security	1027
Appendix	About the CD-ROM	1109
	Index	1113

CONTENTS

	Foreword	xxiii
	Acknowledgments	xxv
	Introduction	xxvii
Chapter 1	Becoming a CISSP	1
	Why Become a CISSP?	1
	The CISSP Exam	2
	CISSP: A Brief History	8
	How Do You Become a CISSP?	8
	Recertification Requirements	9
	What Does This Book Cover?	10
	Tips for Taking the CISSP Exam	10
	How to Use This Book	12
	References	13
	Questions	13
	Answers	17
Chapter 2	Security Trends	19
	How Security Became an Issue	19
	Areas of Security	22
	Benign to Scary	23
	Evidence of the Evolution of Hacking	24
	How Are Nations Affected?	27
	How Are Companies Affected?	29
	The U.S. Government's Actions	31
	So What Does This Mean to Us?	34
	Hacking and Attacking	34
	Management	35
	Internet and Web Activities	37
	Two-Tier Architecture	40
	Database Roles	42
	A Layered Approach	44
	An Architectural View	45
	A Layer Missed	48
	Bringing the Layers Together	48
	Politics and Laws	49
	Education	51
	Summary	52
Chapter 3	Information Security and Risk Management	53
	Security Management	53
	Security Management Responsibilities	54
	The Top-Down Approach to Security	55

Security Administration and Supporting Controls	56
Fundamental Principles of Security	59
Security Definitions	61
Security Through Obscurity	63
Organizational Security Model	65
Security Program Components	67
Business Requirements: Private Industry vs. Military Organizations	80
Information Risk Management	80
Who Really Understands Risk Management?	81
Information Risk Management Policy	82
The Risk Management Team	82
Risk Analysis	83
The Risk Analysis Team	84
The Value of Information and Assets	85
Costs That Make Up the Value	86
Identifying Threats	87
Failure and Fault Analysis	89
Quantitative Risk Analysis	92
Qualitative Risk Analysis	98
Quantitative vs. Qualitative	100
Protection Mechanisms	102
Putting It Together	105
Total Risk vs. Residual Risk	106
Handling Risk	107
Policies, Standards, Baselines, Guidelines, and Procedures	109
Security Policy	110
Standards	112
Baselines	113
Guidelines	114
Procedures	114
Implementation	115
Information Classification	117
Private Business vs. Military Classifications	117
Classification Controls	120
Layers of Responsibility	122
Who's Involved?	123
The Data Owner	130
The Data Custodian	131
The System Owner	131
The Security Administrator	131
The Security Analyst	132
The Application Owner	132
The Supervisor	132
The Change Control Analyst	132
The Data Analyst	133

	The Process Owner	133
	The Solution Provider	133
	The User	134
	The Product Line Manager	134
	The Auditor	134
	Why So Many Roles?	134
	Personnel	135
	Structure	135
	Hiring Practices	136
	Employee Controls	138
	Termination	138
	Security-Awareness Training	139
	Different Types of Security-Awareness Training	140
	Evaluating the Program	141
	Specialized Security Training	142
	Summary	143
	Quick Tips	144
	Questions	147
	Answers	152
Chapter 4	Access Control	155
	Access Controls Overview	155
	Security Principles	156
	Availability	157
	Integrity	157
	Confidentiality	157
	Identification, Authentication, Authorization, and Accountability	158
	Identification and Authentication	160
	Authorization	195
	Access Control Models	210
	Discretionary Access Control	211
	Mandatory Access Control	212
	Role-Based Access Control	214
	Access Control Techniques and Technologies	217
	Rule-Based Access Control	217
	Constrained User Interfaces	218
	Access Control Matrix	219
	Content-Dependent Access Control	221
	Context-Dependent Access Control	221
	Access Control Administration	222
	Centralized Access Control Administration	223
	Decentralized Access Control Administration	230
	Access Control Methods	230
	Access Control Layers	231
	Administrative Controls	232

	Physical Controls	233
	Technical Controls	234
	Access Control Types	237
	Preventive: Administrative	239
	Preventive: Physical	239
	Preventive: Technical	240
	Accountability	243
	Review of Audit Information	245
	Keystroke Monitoring	245
	Protecting Audit Data and Log Information	246
	Access Control Practices	246
	Unauthorized Disclosure of Information	247
	Access Control Monitoring	250
	Intrusion Detection	250
	Intrusion Prevention Systems	260
	A Few Threats to Access Control	263
	Dictionary Attack	263
	Brute Force Attacks	264
	Spoofing at Logon	265
	Summary	269
	Quick Tips	269
	Questions	272
	Answers	276
Chapter 5	Security Architecture and Design	279
	Computer Architecture	281
	The Central Processing Unit	281
	Multiprocessing	286
	Operating System Architecture	287
	Process Activity	294
	Memory Management	296
	Memory Types	298
	Virtual Memory	306
	CPU Modes and Protection Rings	308
	Operating System Architecture	310
	Domains	312
	Layering and Data Hiding	312
	The Evolution of Terminology	314
	Virtual Machines	315
	Additional Storage Devices	317
	Input/Output Device Management	317
	System Architecture	321
	Defined Subsets of Subjects and Objects	322
	Trusted Computing Base	323
	Security Perimeter	326
	Reference Monitor and Security Kernel	327

Security Policy	328
Least Privilege	329
Security Models	330
State Machine Models	331
The Bell-LaPadula Model	333
The Biba Model	336
The Clark-Wilson Model	338
The Information Flow Model	342
The Noninterference Model	345
The Lattice Model	346
The Brewer and Nash Model	348
The Graham-Denning Model	349
The Harrison-Ruzzo-Ulman Model	349
Security Modes of Operation	351
Dedicated Security Mode	352
System High-Security Mode	352
Compartmented Security Mode	352
Multilevel Security Mode	353
Trust and Assurance	355
Systems Evaluation Methods	356
Why Put a Product Through Evaluation?	356
The Orange Book	357
The Orange Book and the Rainbow Series	361
The Red Book	362
Information Technology Security Evaluation Criteria	364
Common Criteria	366
Certification vs. Accreditation	369
Certification	370
Accreditation	371
Open vs. Closed Systems	372
Open Systems	372
Closed Systems	372
Enterprise Architecture	373
A Few Threats to Review	382
Maintenance Hooks	382
Time-of-Check/Time-of-Use Attacks	383
Buffer Overflows	384
Summary	388
Quick Tips	389
Questions	392
Answers	397
Chapter 6 Physical and Environmental Security	401
Introduction to Physical Security	401
The Planning Process	404
Crime Prevention Through Environmental Design	409
Designing a Physical Security Program	414

	Protecting Assets	428
	Internal Support Systems	430
	Electric Power	430
	Environmental Issues	436
	Ventilation	438
	Fire Prevention, Detection, and Suppression	438
	Perimeter Security	446
	Facility Access Control	447
	Personnel Access Controls	454
	External Boundary Protection Mechanisms	455
	Intrusion Detection Systems	464
	Patrol Force and Guards	467
	Dogs	468
	Auditing Physical Access	468
	Testing and Drills	469
	Summary	470
	Quick Tips	470
	Questions	473
	Answers	477
Chapter 7	Telecommunications and Network Security	481
	Open Systems Interconnection Reference Model	483
	Protocol	483
	Application Layer	487
	Presentation Layer	487
	Session Layer	489
	Transport Layer	490
	Network Layer	491
	Data Link Layer	492
	Physical Layer	494
	Functions and Protocols in the OSI Model	494
	Tying the Layers Together	496
	TCP/IP	497
	TCP	498
	IP Addressing	504
	IPv6	505
	Types of Transmission	505
	Analog and Digital	505
	Asynchronous and Synchronous	507
	Broadband and Baseband	507
	LAN Networking	508
	Network Topology	509
	LAN Media Access Technologies	512
	Cabling	519
	Transmission Methods	524
	Media Access Technologies	525
	LAN Protocols	529

Routing Protocols	532
Networking Devices	536
Repeaters	536
Bridges	536
Routers	539
Switches	541
Gateways	545
PBXs	547
Firewalls	548
Honeypot	566
Network Segregation and Isolation	567
Networking Services and Protocols	567
Network Operating Systems	567
Domain Name Service	569
Network Information System	573
Directory Services	575
Lightweight Directory Access Protocol	576
Network Address Translation	577
Intranets and Extranets	579
Metropolitan Area Networks	581
Wide Area Networks	583
Telecommunications Evolution	583
Dedicated Links	586
WAN Technologies	589
Remote Access	603
Dial-Up and RAS	603
ISDN	604
DSL	606
Cable Modems	606
VPN	608
Authentication Protocols	614
Remote Access Guidelines	616
Wireless Technologies	618
Wireless Communications	618
WLAN Components	621
Wireless Standards	623
WAP	635
i-Mode	636
Mobile Phone Security	637
War Driving for WLANs	639
Satellites	640
3G Wireless Communication	641
Rootkits	643
Spyware and Adware	645
Instant Messaging	645
Summary	647

	Quick Tips	647
	Questions	651
	Answers	655
Chapter 8	Cryptography	659
	The History of Cryptography	660
	Cryptography Definitions and Concepts	665
	Kerckhoff's Principle	668
	The Strength of the Cryptosystem	668
	Services of Cryptosystems	669
	One-Time Pad	671
	Running and Concealment Ciphers	673
	Steganography	674
	Governmental Involvement in Cryptography	675
	Types of Ciphers	676
	Substitution Ciphers	677
	Transposition Ciphers	677
	Methods of Encryption	679
	Symmetric vs. Asymmetric Algorithms	679
	Block and Stream Ciphers	685
	Hybrid Encryption Methods	689
	Types of Symmetric Systems	695
	Data Encryption Standard	696
	Triple-DES	703
	The Advanced Encryption Standard	703
	International Data Encryption Algorithm	704
	Blowfish	704
	RC4	705
	RC5	705
	RC6	705
	Types of Asymmetric Systems	706
	The Diffie-Hellman Algorithm	706
	RSA	708
	El Gamal	711
	Elliptic Curve Cryptosystems	712
	LUC	713
	Knapsack	713
	Zero Knowledge Proof	713
	Message Integrity	713
	The One-Way Hash	714
	Various Hashing Algorithms	718
	Attacks Against One-Way Hash Functions	721
	Digital Signatures	722
	Digital Signature Standard	725
	Public Key Infrastructure	725
	Certificate Authorities	726

Certificates	729
The Registration Authority	729
PKI Steps	730
Key Management	732
Key Management Principles	733
Rules for Keys and Key Management	734
Link Encryption vs. End-to-End Encryption	735
E-mail Standards	737
Multipurpose Internet Mail Extension	738
Privacy-Enhanced Mail	738
Message Security Protocol	739
Pretty Good Privacy	739
Quantum Cryptography	741
Internet Security	743
Start with the Basics	743
Attacks	753
Cipher-Only Attack	753
Known-Plaintext Attacks	753
Chosen-Plaintext Attacks	754
Chosen-Ciphertext Attacks	754
Differential Cryptanalysis	755
Linear Cryptanalysis	755
Side-Channel Attacks	755
Replay Attacks	756
Algebraic Attacks	756
Analytic	756
Statistical	757
Summary	757
Quick Tips	758
Questions	761
Answers	765
Chapter 9 Business Continuity and Disaster Recovery	769
Business Continuity and Disaster Recovery	770
Business Continuity Steps	772
Making BCP Part of the Security Policy and Program	774
Project Initiation	776
Business Continuity Planning Requirements	778
Business Impact Analysis	778
Preventive Measures	786
Recovery Strategies	786
Business Process Recovery	788
Facility Recovery	789
Supply and Technology Recovery	795
The End-User Environment	800
Data Backup Alternatives	801

	Electronic Backup Solutions	803
	Choosing a Software Backup Facility	806
	Insurance	808
	Recovery and Restoration	809
	Developing Goals for the Plans	814
	Implementing Strategies	815
	Testing and Revising the Plan	816
	Maintaining the Plan	821
	Summary	825
	Quick Tips	825
	Questions	827
	Answers	832
Chapter 10	Legal, Regulations, Compliance, and Investigations	835
	The Many Facets of Cyberlaw	836
	The Crux of Computer Crime Laws	836
	Complexities in Cybercrime	839
	Electronic Assets	842
	The Evolution of Attacks	842
	Different Countries	844
	Types of Laws	846
	Intellectual Property Laws	849
	Trade Secret	849
	Copyright	850
	Trademark	850
	Patent	851
	Internal Protection of Intellectual Property	851
	Software Piracy	852
	Privacy	853
	Laws, Directives, and Regulations	854
	Employee Privacy Issues	859
	Liability and Its Ramifications	861
	Personal Information	864
	Hacker Intrusion	865
	Investigations	866
	Incident Response	866
	Incident Response Procedures	869
	Computer Forensics and Proper Collection of Evidence	872
	International Organization on Computer Evidence	873
	Motive, Opportunity, and Means	874
	Incident Investigators	875
	The Forensics Investigation Process	876
	What Is Admissible in Court?	880
	Surveillance, Search, and Seizure	883
	Interviewing and Interrogating	884
	A Few Different Attack Types	884

Ethics	888
The Computer Ethics Institute	889
The Internet Architecture Board	890
Corporate Ethics Programs	891
Summary	892
Quick Tips	892
Questions	895
Answers	900
Chapter 11	
Application Security	905
Software's Importance	905
Where Do We Place the Security?	906
Different Environments Demand Different Security	908
Environment vs. Application	908
Complexity of Functionality	909
Data Types, Format, and Length	910
Implementation and Default Issues	910
Failure States	912
Database Management	912
Database Management Software	913
Database Models	914
Database Programming Interfaces	919
Relational Database Components	921
Integrity	924
Database Security Issues	927
Data Warehousing and Data Mining	932
System Development	935
Management of Development	936
Life-Cycle Phases	936
Software Development Methods	950
Computer-Aided Software Engineering	952
Prototyping	953
Change Control	953
The Capability Maturity Model	955
Software Escrow	957
Application Development Methodology	957
Object-Oriented Concepts	958
Data Modeling	966
Software Architecture	966
Data Structures	967
Cohesion and Coupling	967
Distributed Computing	969
CORBA and ORBs	969
COM and DCOM	971
Enterprise JavaBeans	972
Object Linking and Embedding	973
Distributed Computing Environment	974

Expert Systems and Knowledge-Based Systems	975
Artificial Neural Networks	977
Web Security	979
Vandalism	980
Financial Fraud	980
Privileged Access	980
Theft of Transaction Information	981
Theft of Intellectual Property	981
Denial-of-Service (DoS) Attacks	981
Create a Quality Assurance Process	982
Web Application Firewalls	982
Intrusion Prevention Systems	982
Implement SYN Proxies on the Firewall	982
Specific Threats for Web Environments	983
Mobile Code	992
Java	993
ActiveX	995
Malicious Software (Malware)	995
Antivirus Software	1001
Spam Detection	1004
Anti-Malware Programs	1005
Patch Management	1006
Step 1: Infrastructure	1007
Step 2: Research	1007
Step 3: Assess and Test	1007
Step 4: Mitigation (“Rollback”)	1008
Step 5: Deployment (“Rollout”)	1008
Step 6: Validation, Reporting, and Logging	1008
Limitations to Patching	1008
Best Practices	1009
Anything Else?	1009
Attacks	1009
Summary	1014
Quick Tips	1014
Questions	1018
Answers	1023
Chapter 12 Operations Security	1027
The Role of the Operations Department	1028
Administrative Management	1028
Security and Network Personnel	1031
Accountability	1032
Clipping Levels	1033
Assurance Levels	1034
Operational Responsibilities	1034
Unusual or Unexplained Occurrences	1035

Deviations from Standards	1035
Unscheduled Initial Program Loads (a.k.a. Rebooting)	1036
Asset Identification and Management	1036
System Controls	1037
Trusted Recovery	1038
Input and Output Controls	1040
System Hardening	1042
Remote Access Security	1044
Configuration Management	1045
Change Control Process	1045
Change Control Documentation	1047
Media Controls	1048
Data Leakage	1054
Network and Resource Availability	1056
Mean Time Between Failures (MTBF)	1057
Mean Time to Repair (MTTR)	1058
Single Points of Failure	1058
Backups	1066
Contingency Planning	1070
Mainframes	1070
E-mail Security	1072
How E-mail Works	1074
Facsimile Security	1076
Hack and Attack Methods	1078
Vulnerability Testing	1087
Penetration Testing	1090
Wardialing	1094
Other Vulnerability Types	1095
Postmortem	1097
Summary	1099
Quick Tips	1099
Questions	1101
Answers	1106
Appendix	
About the CD-ROM	1109
Running the QuickTime Cryptography Video Sample	1110
Troubleshooting	1111
Installing Total Seminars' Test Software	1111
Navigation	1111
Practice Mode	1111
Final Mode	1111
Minimum System Requirements for Total Seminars'	
Software	1112
Technical Support	1112
Index	1113