Contents

Foreword xcv
Introduction xxix
Assessment Test 1

Chapter 1 Measuring and Weighing Risk 1
Risk Assessment 2
  Computing Risk Assessment 3
  Acting on Your Risk Assessment 5
  Risks Associated with Cloud Computing 7
  Risks Associated with Virtualization 8
Developing Policies, Standards, and Guidelines 9
  Implementing Policies 9
  Incorporating Standards 10
  Following Guidelines 11
  Business Policies 12
  Understanding Control Types, False Positives, and Change and Incident Management 16
Summary 18
Exam Essentials 19
Review Questions 20
Answers to Review Questions 24

Chapter 2 Infrastructure and Connectivity 27
Mastering TCP/IP 29
  Working with the TCP/IP Suite 30
  IPv4 vs. IPv6 33
  Understanding Encapsulation 34
  Working with Protocols and Services 35
Distinguishing between Security Topologies 41
  Setting Design Goals 41
  Creating Security Zones 43
  Working with Newer Technologies 48
  Working with Business Requirements 53
Understanding Infrastructure Security 53
  Working with Hardware Components 53
  Working with Software Components 55
Understanding the Different Network Infrastructure Devices 56
  Firewalls 56
  Hubs 61
  Modems 62
Chapter 5  Access Control and Identity Management  175

Access Control Basics  177
   Identification vs. Authentication  177
   Authentication (Single Factor) and Authorization  178
   Multifactor Authentication  178
   Operational Security  180
   Tokens  180
   Potential Authentication and Access Problems  181
   Authentication Issues to Consider  182

Understanding Remote Access Connectivity  184
   Using the Point-to-Point Protocol  184
   Working with Tunneling Protocols  185
   Working with RADIUS  186
   TACACS/TACACS+/XTACACS  187
   VLAN Management  187

Understanding Authentication Services  189
   LDAP  189
   Kerberos  189
   Single Sign-On Initiatives  189
# Contents

- Understanding Quantum Cryptography 299
- Uncovering the Myth of Unbreakable Codes 300
- Understanding Cryptographic Algorithms 302
  - The Science of Hashing 302
  - Working with Symmetric Algorithms 304
  - Working with Asymmetric Algorithms 307
- Wi-Fi Encryption 309
- Using Cryptographic Systems 309
  - Confidentiality 310
  - Integrity 310
  - Digital Signatures 311
  - Authentication 312
  - Non-repudiation 314
  - Access Control 314
- Key Features 315
- Understanding Cryptography Standards and Protocols 315
  - The Origins of Encryption Standards 316
  - Public-Key Infrastructure X.509/Public-Key Cryptography Standards 320
    - X.509 321
    - SSL and TLS 321
    - Certificate Management Protocols 323
    - Secure Multipurpose Internet Mail Extensions 323
    - Secure Electronic Transaction 324
    - Secure Shell 325
    - Pretty Good Privacy 325
    - HTTP Secure 327
    - Secure HTTP 327
    - IP Security 327
    - Tunneling Protocols 330
    - Federal Information Processing Standard 330
- Summary 331
- Exam Essentials 331
- Review Questions 333
- Answers to Review Questions 337

---

## Chapter 9 Cryptography Implementation 339

- Using Public Key Infrastructure 340
  - Using a Certificate Authority 341
  - Working with Registration Authorities and Local Registration Authorities 342
- Implementing Certificates 344
- Understanding Certificate Revocation 347
- Implementing Trust Models 348
Secure Network Administration Principles 409
   Rule-Based Management 410
   Port Security 410
   Working with 802.1X 411
   Flood Guards and Loop Protection 411
   Preventing Network Bridging 411
   Log Analysis 412
Mitigation and Deterrent Techniques 412
   Manual Bypassing of Electronic Controls 412
   Monitoring System Logs 413
   Security Posture 419
   Reporting 420
   Detection/Prevention Controls 420
Summary 421
Exam Essentials 421
Review Questions 422
Answers to Review Questions 426

Chapter 12 Wireless Networking Security 429
Working with Wireless Systems 430
   IEEE 802.11x Wireless Protocols 430
   WEP/WAP/WPA/WPA2 432
   Wireless Transport Layer Security 434
Understanding Mobile Devices 435
   Wireless Access Points 436
   Extensible Authentication Protocol 441
   Lightweight Extensible Authentication Protocol 442
   Protected Extensible Authentication Protocol 443
Wireless Vulnerabilities to Know 443
Summary 448
Exam Essentials 448
Review Questions 450
Answers to Review Questions 454

Chapter 13 Disaster Recovery and Incident Response 455
Understanding Business Continuity 456
   Undertaking Business Impact Analysis 457
   Utilities 458
   High Availability 460
   Disaster Recovery 464
   Incident Response Policies 479
   Understanding Incident Response 480
   Succession Planning 487
Contents

Chapter 14 Security-Related Policies and Procedures

Policies You Must Have
  Data Loss/Theft Policies 500
  Least Privilege 501
  Separation of Duties 502
  Time of Day Restrictions 502
  Mandatory Vacations and Job Rotation 504
Policies You Should Have
  Human Resource Policies 504
  Certificate Policies 508
Security Controls for Account Management
  User and Group Role Management 510
  Users with Multiple Accounts/Roles 512
  Auditing 512
  Account Policy Enforcement 519
Summary 521
Exam Essentials 522
Review Questions 523
Answers to Review Questions 527

Chapter 15 Security Administration

Security Administrator’s Troubleshooting Guide 530
Getting Started 531
  Creating a Home Lab 531
  In the Workplace 532
  Which OS Should You Use? 533
  Creating a Security Solution 533
Access Control Issues 534
Accountability Concerns 534
Auditing 535
Authentication Schemes 536
  Authentication Factors 536
  Mutual Authentication 537
  Authentication Protection 538
Backup Management 538
Contents

Baselining Security 539
Certificate Management 540
Communications Security 541
  Preauthentication 541
  Remote Control/Remote Shell 542
  Virtual Private Networks 543
Directory Services Protection 543
Disaster Planning 544
Documenting Your Environment 545
Email Issues 545
File-Sharing Basics 547
Working with IDSs and Honey Pots 548
Incident Handling 548
Internet Common Sense 549
Key Management Conventions 550
Preventing Common Malicious Events 551
  Constructing a Line of Defense 552
  Types of Attacks 553
  Antivirus Protection 554
  Making Stronger Passwords 555
Managing Personnel 557
Keeping Physical Security Meaningful 558
Securing the Infrastructure 560
Working with Security Zones 562
Social Engineering Risks 562
System Hardening Basics 563
Securing the Wireless Environment 565
Summary 566

Appendix A About the Companion CD 567

What You'll Find on the CD 568
  Sybex Test Engine 568
  Electronic Flashcards 568
  PDF of the Glossary 568
System Requirements 569
Using the CD 569
Troubleshooting 570
  Customer Care 570

Glossary 571

Index 613