

DESIGNING NETWORK SECURITY, 2ND EDITION

Introduction.

I. SECURITY FUNDAMENTALS.

1. Basic Cryptography.

Cryptography. Authentication and Authorization. Namespace. Key Management. Key Escrow. Summary. Review Questions.

2. Security Technologies.

Identity Technologies. Application Layer Security Protocols. Transport Layer Security Protocols. Network Layer Security. Link-Layer Security Technologies. Public Key Infrastructure and Distribution Models. Summary. Review Questions.

3. Applying Security Technologies to Real Networks.

Virtual Private Networks (VPNs). Wireless Networks. Voice over IP (VoIP) Networks. Summary. Review Questions.

4. Routing Protocol Security.

Routing Basics. Routing Protocol Security Details. Summary. Review Questions.

II. THE CORPORATE SECURITY POLICY.

5. Threats in an Enterprise Network.

Types of Threats. Motivation of Threat. Common Protocol Vulnerabilities. Common Network Scenario Threats and Vulnerabilities. Routing Protocols. Social Engineering. Summary. Review Questions.

6. Considerations for a Site Security Policy.

Where to Begin. Risk Management. A Security Policy Framework. Summary. Review Questions.

7. Design and Implementation of the Corporate Security Policy.

Physical Security Controls. Logical Security Controls. Infrastructure and Data Integrity. Data Confidentiality. Security Policy Verification and Monitoring. Policies and Procedures for Staff. Security Awareness Training. Summary. Review Questions.

8. Incident Handling.

Building an Incident Response Team. Detecting an Incident. Handling an Incident. Incident Vulnerability Mitigation. Responding to the Incident. Recovering from an Incident. Summary. Review Questions.

III. PRACTICAL IMPLEMENTATION.

9. Securing the Corporate Network Infrastructure.

Identity - Controlling Network Device Access. Integrity. Data Confidentiality. Network Availability. Audit. Implementation Examples. Summary. Review Questions.

10. Securing Internet Access.

Internet Access Architecture. External Screening Router Architecture. Advanced Firewall Architecture. Implementation Examples. Summary. Review Questions.

BUY ONLINE AT: <http://www.itgovernance.co.uk/products/727>

11. Securing Remote Dial-In Access.

Dial-In Security Concerns. Authenticating Dial-In Users and Devices. Authorization. Accounting and Billing. Using AAA with Specific Features. Encryption for Virtual Dial-In Environments. Summary. Review Questions.

12. Securing VPN, Wireless, and VoIP Networks.

Virtual Private Networks. Wireless Networks. Voice over IP Networks. Summary. Review Questions.

IV. APPENDIXES.

Appendix A: Sources of Technical Information.

Appendix B: Reporting and Prevention Guidelines: Industrial Espionage and Network Intrusions.

Appendix C: Port Numbers.

Appendix D: Mitigating Distributed Denial-of-Service Attacks.

Appendix E: Answers to Review Questions.

Glossary.

Index.