1. Record Nr. UNINA9910154775303321

Autore	Boyle Randall
Titolo	Corporate computer security [[electronic resource] /] / Randall J. Boyle, Raymond R. Panko
Pubbl/distr/stampa	Boston : , : Pearson, , [2015] ©2015
ISBN	1-292-06659-8
Edizione	[Fourth, Global edition.]
Descrizione fisica	1 online resource (672 pages) : illustrations, graphs
Collana	Always Learning
Disciplina	005.8
Soggetti	Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Cover -- Contents -- Preface -- About the Authors -- Chapter 1: The Threat Environment -- 1.1 Introduction -- Basic Security Terminology -- The Threat Environment -- Security Goals -- Compromises -- CounterMeasures -- 1.2 Employee and Ex-Employee Threats -- Why Employees are Dangerous -- Employee Sabotage -- Employee Hacking -- Employee Financial Theft and Theft of Intellectual Property -- Employee Extortion -- Employee Sexual or Racial Harassment -- Employee Computer and Internet Abuse -- Internet Abuse -- Non-Internet Computer Abuse -- Data Loss -- Other "Internal" Attackers -- 1.3 Malware -- Malware Writers -- Viruses -- Worms -- Blended Threats -- Payloads -- Trojan Horses and Rootkits -- Nonmobile Malware -- Trojan Horses -- Remote Access Trojans -- Downloaders -- Spyware -- Rootkits -- Mobile Code -- Social Engineering in Malware -- Spam -- Phishing -- Spear Phishing -- Hoaxes -- 1.4 Hackers and Attacks -- Traditional Motives -- Anatomy of a Hack -- Target Selection -- Reconnaissance Probes -- The Exploit -- Spoofing -- Social Engineering in an Attack -- Denial-of-Service Attacks -- Skill Levels -- 1.5 The Criminal Era -- Dominance by Career Criminals -- Cybercrime -- International Gangs -- Black Markets and Market Specialization -- Fraud, Theft, and Extortion -- Fraud -- Financial and Intellectual Property Theft -- Extortion Against Corporations -- Stealing Sensitive Data about Customers and Employees -- Carding -- Bank Account Theft -- Online Stock Account Theft -- Identity Theft --

The Corporate Connection -- Corporate Identity Theft -- 1.6 Competitor Threats -- Commercial Espionage -- Denial-of-Service Attacks -- 1.7 Cyberwar and Cyberterror -- Cyberwar -- Cyberterror -- 1.8 Conclusion -- Thought Questions -- Hands-on Projects -- Project Thought Questions -- Case Study -- Case Discussion Questions -- Perspective Questions.
Chapter 2: Planning and Policy -- 2.1 Introduction -- Defense -- Management Processes -- Management is the Hard Part -- Comprehensive Security -- Weakest-Links Failures -- The Need to Protect Many Resources -- The Need for a Disciplined Security Management Process -- The Plan-Protect-Respond Cycle -- Planning -- Protection -- Response -- Vision in Planning -- Viewing Security as an Enabler -- Developing Positive Visions of Users -- Strategic IT Security Planning -- 2.2 Compliance Laws and Regulations -- Driving Forces -- Sarbanes-Oxley -- Privacy Protection Laws -- Data Breach Notification Laws -- The Federal Trade Commission -- Industry Accreditation -- PCI-DSS -- FISMA -- 2.3 Organization -- Chief Security Officers -- Should You Place Security within IT? -- Locating Security Within It -- Placing Security Outside It -- A Hybrid Solution -- Top Management Support -- Relationships with Other Departments -- Special Relationships -- All Corporate Departments -- Business Partners -- Outsourcing IT Security -- E-mail Outsourcing -- Managed Security Service Provider -- 2.4 Risk Analysis -- Reasonable Risk -- Classic Risk Analysis Calculations -- Asset Value -- Exposure Factor -- Single Loss Expectancy -- Annualized Probability (or Rate) of Occurrence -- Annualized Loss Expectancy -- Countermeasure Impact -- Annualized Countermeasure Cost and Net Value -- Problems with Classic Risk Analysis Calculations -- Uneven Multiyear Cash Flows -- Total Cost of Incident -- Many-To-Many Relationships Between Countermeasures and Resources -- The Impossibility of Computing Annualized Rates of Occurrence -- The Problem With "Hard-Headed Thinking" -- Perspective -- Responding to Risk -- Risk Reduction -- Risk Acceptance -- Risk Transference (Insurance) -- Risk Avoidance -- 2.5 Technical Security Architecture -- Technical Security Architectures -- Architectural Decisions.
Dealing With Legacy Security Technology -- Principles -- Defense in Depth -- Defense in Depth Versus Weakest Links -- Single Points of Vulnerability -- Minimizing Security Burdens -- Realistic Goals -- Elements of a Technical Security Architecture -- Border Management -- Internal Site Security Management -- Management of Remote Connections -- Interorganizational Systems -- Centralized Security Management -- 2.6 Policy-Driven Implementation -- Policies -- What are Policies? -- What, Not How -- Clarity -- Categories of Security Policies -- Corporate Security Policy -- Major Policies -- Acceptable Use Policy -- Policies for Specific Countermeasures or Resources -- Policy-Writing Teams -- Implementation Guidance -- No Guidance -- Standards and Guidelines -- Types of Implementation Guidance -- Procedures -- Processes -- Baselines -- Best Practices and Recommended Practices -- Accountability -- Ethics -- Exception Handling -- Oversight -- Policies and Oversight -- Promulgation -- Electronic Monitoring -- Security Metrics -- Auditing -- Anonymous Protected Hotline -- Behavioral Awareness -- Fraud -- Sanctions -- 2.7 Governance Frameworks -- Coso -- The Coso Framework -- Objectives -- Reasonable Assurance -- Coso Framework Components -- CobiT -- The Cobit Framework -- Dominance in the United States -- The ISO/IEC 27000 Family -- ISO/IEC 27002 -- ISO/IEC 27001 -- Other 27000 Standards -- 2.8 Conclusion -- Thought Questions -- Hands-on Projects -- Project Thought Questions -- Case Study -- Case

Discussion Questions -- Perspective Questions -- Chapter 3: Cryptography -- 3.1 What is Cryptography? -- Encryption for Confidentiality -- Terminology -- Plaintext -- Encryption and Ciphertext -- Cipher -- Key -- Keeping the Key Secret -- The Simple Cipher -- Cryptanalysis -- Substitution and Transposition Ciphers -- Substitution Ciphers -- Transposition Ciphers.
Real-world Encryption -- Ciphers and Codes -- Symmetric Key Encryption -- Key Length -- Human Issues in Cryptography -- 3.2 Symmetric Key Encryption Ciphers -- RC4 -- The Data Encryption Standard (DES) -- 56-Bit Key Size -- Block Encryption -- Triple DES (3DES) -- 168-Bit 3DES Operation -- 112-Bit 3DES -- Perspective on 3DES -- Advanced Encryption Standard (AES) -- Other Symmetric Key Encryption Ciphers -- 3.3 Cryptographic System Standards -- Cryptographic Systems -- Initial Handshaking Stages -- Negotiation -- Initial Authentication -- Keying -- Ongoing Communication -- 3.4 The Negotiation Stage -- Cipher Suite Options -- Cipher Suite Policies -- 3.5 Initial Authentication Stage -- Authentication Terminology -- Hashing -- Initial Authentication with MS-CHAP -- On The Supplicant's Machine: Hashing -- On The Verifier Server -- 3.6 The Keying Stage -- Session Keys -- Public Key Encryption for Confidentiality -- Two Keys -- Process -- Padlock and Key Analogy -- High Cost and Short Message Lengths -- RSA and ECC -- Key Length -- Symmetric Key Keying Using Public Key Encryption -- Symmetric Key Keying Using Diffie-Hellman Key Agreement -- 3.7 Message-By-Message Authentication -- Electronic Signatures -- Public Key Encryption for Authentication -- Message-by-Message Authentication with Digital Signatures -- Digital Signatures -- Hashing to Produce the Message Digest -- Signing the Message Digest to Produce the Digital Signature -- Sending the Message with Confidentiality -- Verifying the Supplicant -- Message Integrity -- Public Key Encryption for Confidentiality and Authentication -- Digital Certificates -- Certificate Authorities -- Digital Certificate -- Verifying the Digital Certificate -- The Roles of the Digital Certificate and Digital Signature -- Key-Hashed Message Authentication Codes -- The Problem with Digital Signatures.
Creating and Testing the HMAC -- Nonrepudiation -- 3.8 Quantum Security -- 3.9 Cryptographic Systems -- Virtual Private Networks (VPNs) -- Why VPNs? -- Host-to-Host VPNs -- Remote Access VPNs -- Site-to-Site VPNs -- 3.10 SSL/TLS -- Nontransparent Protection -- Inexpensive Operation -- SSL/TLS Gateways and Remote Access VPNs -- VPN Gateway Standards -- Authentication -- Connecting the Client PC to Authorized Resources -- Security for Services -- Browser on the Client -- Advanced Services Require Administrator Privileges on PCs -- Perspective -- 3.11 IPsec -- Attractions of IPsec -- SSL/TLS Gives Nontransparent Transport Layer Security -- IPsec: Transparent Internet Layer Security -- IPsec in Both IPv4 and IPv6 -- IPsec Transport Mode -- Host-To-Host Security -- End-To-End Protection -- Cost of Setup -- IPsec in Transport Mode and Firewalls -- IPsec Tunnel Mode -- Protection is Provided by IPsec Gateways -- Less Expensive than Transport Mode -- Firewall-Friendly Protection -- No Protection within the Two Sites -- IPsec Security Associations (SAs) -- Separate SAs in the Two Directions -- Policy-Based SA -- 3.12 Conclusion -- Thought Questions -- Hands-on Projects -- Project Thought Questions -- Case Study -- Case Discussion Questions -- Perspective Questions -- Chapter 4: Secure Networks -- 4.1 Introduction -- Creating Secure Networks -- Availability -- Confidentiality -- Functionality -- Access Control -- Future of Secure Networks -- Death of the Perimeter -- Rise of the City -- 4.2 DoS Attacks -- Denial of Service. . . But Not an Attack -- Faulty Coding -- Referrals from Large Sites -- Goal of DoS Attacks

-- Stop Critical Services -- Degrade Services -- Methods of DoS Attacks -- Direct and Indirect Attacks -- Intermediary -- Reflected Attack -- Sending Malformed Packets -- Defending Against Denial-of-Service Attacks -- Black Holing.
Validating the Handshake.

Sommario/riassunto

For introductory courses in IT Security. A strong business focus through a solid technical presentation of security tools. Corporate Computer Security provides a strong business focus along with a solid technical understanding of security tools. This text gives students the IT security skills they need for the workplace. This edition is more business focused and contains additional hands-on projects, coverage of wireless and data security, and case studies. This program will provide a better teaching and learning experience-for you and your students. Here's how: Encourage Student's to Apply Concepts: Each chapter now contains new hands-on projects that use contemporary software. Business Environment Focus: This edition includes more of a focus on the business applications of the concepts. Emphasis has been placed on securing corporate information systems, rather than just hosts in general. Keep Your Course Current and Relevant: New examples, exercises, and research findings appear throughout the text.