Information Security
Management Handbook

introduction

Sixth Edition

Section - >

htoq xj isifiti/n bU;jii-iij \^ojuoa bab: _^ 

"olttaroid F Tiptbn, CISSP; Midki KraitSevCisSEi

icft fino bwu sis birfi ;

A Auerbach Publications , nl?cAp^n
A ^ j \ Taylor & Francis Group • Slb-b—8 200

Auerbach Publications is an imprint of the Taylor & Francis Group, an informa business
# Table of Contents

Introduction .................................................. xxiii

Editors .......................................................... xxv

Contributors .................................................... xxvii

1 INFORMATION SECURITY AND RISK MANAGEMENT

Section 1.1 Security Management Concepts and Principles

1 Bits to Bytes to Boardroom .................................. 9
   Micki Krause

2 Information Security Governance ............................ 15
   Todd Fitzgerald

3 Corporate Governance ....................................... 35
   David C. Krehk

4 IT Governance Institute (ITGI) Overview .................. 45

5 Top Management Support Essential for Effective Information Security ................................. 51
   Kenneth J. Knapp and Thomas E. Marsh

6 Managing Security by the Standards: An Overview and Primer .............................................. 59
  Bonnie A. Coins

7 Information Security for Mergers and Acquisitions ............................................................. 67
  Craig A. Schiller

8 Information Security Governance ............................ 89
   Ralph Spertifoor

 Belts and Suspenders: Diversity in Information Technology Security ........................................ 95
   Bari
Section 1.2 Change Control Management

16 Patch Management 101: It Just Makes Good Sense! .......................... Lynda L. McGhie

17 Security Patch Management: The Process ...................................... 185 Felicia M. Nicastro

18 Configuration Management: Charting the Course for the Organization ................................. 201 Mollie E. Krehnke and David C. Krehnke

Section 1.3 Data Classification

19 Information Classification: A Corporate Implementation Guide ............... 221 Jim Appleyard

20 Ownership and Custody of Data .................................................. 233 William Hugh Murray

Section 1.4 Risk Management

21 Information Security Risk Assessment ........................................... 243 Samantha Thomas Cruz

22 Developing and Conducting a Security Test and Evaluation .................. 251 Sean M. Price

23 Enterprise Security Management Program ..................................... 261 George G. McBride
24 Technology Convergence and Security: A Simplified Risk Management Model. Km M. Shaurette


26 A Matter of Trust. Ray Kaplan

27 Trust Governance in a Web Services World. Daniel D. Houser

28 Risk Management and Analysis. Kevin Henr

29 New Trends in Information Risk Management. Brett Regan Young


Section 1.5 Policies, Standards, Procedures and Guidelines

31 Committee of Sponsoring Organizations (COSO)


34 People, Processes, and Technology. Felicia M. Nicastr

35 Building an Effective Privacy Program. Rebecca Herold

36 Establishing an E-Mail Retention Policy: Preventing Potential Legal Nightmares. D. Fried

37 Ten Steps to Effective Web-Based Security Policy Development and Distribution. Fitzgerald
Section 1.6 Security Awareness Training

43 Change That Attitude: The ABCs of a Persuasive Security Awareness Program .......................... 521
W. Chun

44 Maintaining Management’s Commitment .............................................................. 531
William Tompkins

45 Making Security Awareness Happen .................................................................. 541
Susan D. Hansche

46 Beyond Information Security Awareness Training: It Is Time
To Change the Culture ......................................................................................... 555
Stan Stahl

Section 1.7 Security Management Planning

47 Overview of an IT Corporate Security Organization ............................................. 567
Jeffrey Davis

48 Make Security Part of Your Company’s DNA ....................................................... 579
Ken M. Shaurette

49 Building an Effective and Winning Security Team ............................................. 591
Lynda L McGhie

50 When Trust Goes Beyond the flordqn.Mpvg XQU&fieyeJ.opmejrt, „
Work Offshore .................................................................................................... 607
Stephen D. Fried
Section 1.8  Ethics

56  Ethics and the Internet ............................................. 673
    Micki Krause

57  Computer
    Peter S. Tippett

Section 2.1  Access Control Techniques

58  A Look at RFID Security ............................................ 715
    Ben Rothke

59  New Emerging Information Security Technologies and Solutions ............................................. 739
    Tara Chand

60  Sensitive or Critical Data Access Control............................................. 739
    Mollie E. Krehnke and David C. Krehnke

61  An Introduction to Role-Based Access Control ............................................. 751
    Ian Clark

62  Smart Cards ............................................. 765
    James S. Tiller

63  A Guide to Evaluating Tokens ............................................. 775
    Joseph T. Hootman

64  Controlling FTP: Providing Secured Data Transfers ............................................. 785
    Chris Hare
Section 2.2 Access Control Administration

65 End Node Security and Network Access Management: Deciding Among Different Strategies .................................................. 803
Franjo Majster

66 Identity Management: Benefits and Challenges, ....."","","","","","",# ... w ... 823
I. McGrie

67 Blended Threat Analysis: Passwords and Policy ,,*",",",",",",","",","",","",","",","",",","",","",","",","",","",","",","",","",",","",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",",","'}

Section 2.3 Identification and Authentication Techniques 

68 Enhancing Security through Biometric Technology ......... 869
Stephen D. Fried

69 Single Sign-On for the Enterprise ........................................ 887
Ross A. Leo

Section 2.4 Access Control Methodologies and Implementation

70 Centralized Authentication Services (RADIUS, TACACS, DIAMETER) ............................................................... 909
Bilistackpole

71 An Introduction to Secure Remote Access ............... 92;

Section 2.5 Methods of Attack

72 Hacker Tools and Techniques 'JffWW?. WtWCO'iohiJ.aWSPCJ^ y «W.. PA . . 935
Sloodu

73 A New Breed of Hacker Tools and Defenses ......... MiO. W.T'ItiftQ&. PA . . 951
Ed Sloewfęc

74 Hacker Attacks and Defend 2 .,<^>pAl^Kr9.-?lV a A^ RQJ^H^ojjnl.nA.. J A . . 965
Ed Skoudis

75 Counter-Economic Espionage .......................... i..i..*ite£J?iR&M. . . 977
Craig A. Schiller

Section 2.6 Monitoring and Penetration Testing

76 Insight into Intrusion Prevention System*liiwwfl.:KT3. SAIUtVloU.. M . . 993
Deograt-Lumy and Roy Naldo
3 CRYPTOGRAPHY

Section 3.1 Use Of C

78 Auditing Cryptography: Assessing System Security ................. 1023
Steve Stanek

Section 3.2 Cryptographic Concepts, Methodologies, and Practices

79 Cryptographic Transitions
Spencer Poore

80 Blind Detection of Steganographic Content in Digital Images
Using Cellular Automata .................................................. 1039
Sasan Hamidi

81 An Overview of Quantum Cryptography ................................ 1045
Ben Rothke

82 Elliptic Curve Cryptography: Delivering High-Performance
Security for E-Commerce and Communications ........................ 1059
Paul Lambert

83 Cryptographic Key Management Concepts
Spencer Poore

84 Message Authentication .............................................. 1067
Tiller

85 Fundamentals of Cryptography and Encryption ........................ 1095
Ronald A. Gave

86 Steganography: The Arj^iuig Messages
Markhdmead

87 An Introduction to Cryptography

88 Hash

89 A Look at the Advanced Encryption Standard
Ben Rothke
Section 3.3 Private Key Algorithms

90 Principles and Applications of Cryptographic Key Management ............................................. 1159
William Hugh Murray

Section 3.4 Public Key Infrastructure (PKI)

91 Preserving Public Key Hierarchy .......................................................... 1175
Geoffrey C. Grabow

92 PKI Registration .......................................................... 1183
Alex Golod

Section 3.5 System Architecture for Implementing Cryptographic Functions

93 Implementing Kerberos in Distributed Systems .................................................. 1197
Joe Kovara and Ray Kaplan

Section 3.6 Methods of Attack

94 Methods of Attacking and Defending Cryptosystems ............................................. 1255
Joost Houwen

4 PHYSICAL (ENVIRONMENTAL) SECURITY ...................... 1271

Section 4.1 Elements of Physical Security

95 Perimeter Security .......................................................... 1275
R. Scott McCoy

96 Melding Physical Security and Traditional Information Systems Security .......................................................... 1289
Kevin Henry

97 Physical Security for Mission-Critical Facilities and Data Centers ............................................. 1293
Gerald Bowman

98 Physical Security: A Foundation for Information Security ............................................. 1317
Christopher Steinke

99 Physical Security: Controlled Access and Layered Defense ............................................. 1327
Bruce R. Matthews

100 Computing Facility Physical Security .......................................................... 1339
Alan Brusewitz
Section 4.2 Technical Controls

Types of Information Security Controls .................................................. 1357
Harold F. Tipton

Section 4.3 Environment and Prevention

Workplace Violence: Event Characteristics and Prevention ........................................ 1367
George Richards

Physical Security: The Threat after September 11, 2001 ....................................... 1373
Jaymes Williams

5 SECURITY ARCHITECTURE AND DESIGN

Section 5.1 Principles of Computer and Network Organizations, Architectures, and Designs

Enterprise Assurance: A Framework Explored.................................................. 1387
Bonnie A. Goins

Creating a Secure Architecture................................................................. 1403
Christopher A. Pilewski and Bonnie A. Goins

Common Models, for Architecting an Enterprise Security.................................. 1413
Matthew J. Decker

The Reality of Virtual Computing......................................................................... 1431
Chris Hare

Section 5.2 Principles of Security Models, Architectures and Evaluation Criteria

Formulating all Enterprise Inforamidfi-ii<89aKA|3i:qmU33ni2ua9HT  IZI
Security Architecture v-lwakAWwWQffM^WM^WnJmQ^OKV.LI1  .......................... 1451
Mollie E. Krehnke and David C. Krehnke

Security Architecture and Models ................................................................. 1469
Foster J. Henderson and Kellina M. Craig-Henderson

The Common Criteria for IT Security Evaluation .............................................. 1487
Debra S. Herrmann
Common Flaws and Security Issues: System Architecture and Design

William Hugh Murray

6 BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY PLANNING

Business Continuity Planning

Developing Realistic Continuity Planning Process Metrics
Carl B. Jackson

Building Maintenance Processes for Business Continuity Plans
Ken Doughty

Identifying Critical Business Functions
Bonnie A. Goins

Selecting the Right Business Continuity Strategy
Ken Doughty

Contingency Planning Best Practices and Program Maturity
Timothy R. Stacey

Reengineering the Business Continuity Planning Process
Carl B. Jackson

The Role of Continuity Planning in the Enterprise Risk Management Structure
Carl B. Jackson

Disaster Recovery Planning

Contingency at a Glance
Ken M. Shaurette and Thomas J. Schleppenbach

The Business Impact Assessment Process and the Importance of Using Business Process Mapping
Carl B. lacfson

Testing Business Continuity and Disaster Recovery Plans
James S. Mitts

Restoration Component of Business Continuity Planning
John Dorfand Martin Johnson
Business Resumption Planning and Disaster Recovery. A Case History. Kevin Henry 1655

Business Continuity Planning: A Collaborative Approaches. Kevin Henry 1665

Section 6.3 Elements of Business Continuity Planning

The Business Continuity Planning Framework. 1675

7 TELECOMMUNICATIONS AND NETWORK SECURITY

Section 7.1 Communications and Network Security


The Five W's and Designing a Secure, Identity-Based, Self-Defending Network. Samuel W. Chun 1721

Maintaining Network Security: Availability via Intelligent Agents. Robby Fussell 1731

PBXFirewalls: Closing the Back Door. William A. Yarberry, Jr. 1739

Network Security Overview. Bonnie A. Goins and Christopher A. Pilewski 1751

Putting Security in the Transport: TLS'. Chris Hare 1761

WLAN Security Update. Franjo Majstor 1777

Understanding SSL. Chris Hare 1791

Packet Sniffers and Network Monitoring. S. Ti/ter and Bryan D. Fish 1811

Secured Connections to External Networks. Steven F. Blanding 1827

Security and Network Technologies. Chris Hare 1843
Wired and Wireless Physical Layer Security Issues

Network Router Security

What's Not So Simple about SNMP?

ISO/OSI and TCP/IP Network Model Characteristics

VoIP Security Issues

An Examination of Firewall Architectures

Voice over WLAN

Spam Wars: How To Deal with Junk E-Mail

Secure Web Services: Holes and Fillers

IPSec Virtual Private Networks

Internet Security: Securing the Perimeter

Application-Layer Security - Protocols for

Application Layer: Next Level
Section 7.3 E-mail Security

160 Instant Messaging Safety

William Hugh Murray

Section 7.4 Secure Voice Communications

161 VokeSecurity

Chris Hare

162 Secure Voice Communications (Vol)

Valene Skerpac

Section 7.5 Network Attacks and Countermeasures

163 Deep Packet Inspection Technologies

Anderson Ramos

164 Wireless Penetration Testing: Case Study and Countermeasures

Christopher A. Pilewski

165 Auditing the Telephony System: Defenses against Communications

Security Breaches and Toll Fraud

166 Insecurity by Proxy

Micuh. Silverman

167 Wireless Security
8 APPLICATION SECURITY ........................................ 263

Section 8.1 Application Issues «^H,", "» J

170 Application Service Provider Security: Ensuring a Secure Relationship for the Client and the ASP .................................................. 2267
   Stephen D. Fried

171 Stack-Based Buffer Overflows ........................................ 2289
   Jonathan S. Held

172 Web Application Security .............................................. 2301
   Mandy Andress

173 Security for XML and Other Metadata Languages ........................................ 2311
   William Hugh Murray

174 XML and Information Security ........................................... 2319
   Samuel C. McClintock

175 Application Security .................................................. 2327
   Walter S. Kobus, Jr.

176 Covert Channels .......................................................... 2335
   Anton Chuvakin

177 Security as a Value Enhancer in Application Systems Development ........................................ 2343
   Lowell Bruce McCulley

178 Open Source versus Closed Source ........................................ 2361
   Eli Skoudis

179 A Look at Java Security .................................................. 2381
   Ben Rothke

Section 8.2 Databases and Data Warehousing

180 Reflections on Database Integrity ........................................ 2387
   William Hugh Murray

181 Digital Signatures in Relational Database Applications ........................................ 2395
   Mike R. Prevost
Section 8.3 Systems Development Controls


George G. McBride

Avoiding Buffer Overflow Attacks

Sean M. Price

Secure Development Life Cycle

Kevin Henry

System Development Security Methodology

Ian Lim and Ioana V. Bazavan

Software Engineering Institute Capability Maturity Model

Matt Nelson

Enterprise Security Architecture

William Hugh Murray

Certification and Accreditation Methodology

E. ide&Hte ami David C. Krehnke

System Development Security Methodology

Ian Lim and Ioana V. Bazavan

Methods of Auditing Applications

David C. Rice and Graham Bucholz

Section 8.4 Methods of Attack

Enabling Safer Deployment of Internet Mobile Code

Ron Moritz

9 OPERATIONS SECURITY

Security Considerations in Distributed Computing: A Grid

Sasan Hamidi
195 Managing Unmanaged Systems .................................................. 2579
    Bill Stackpole and Man Nguyen

196 Storage Area Networks Security Protocols and Mechanisms .............. 2597
    Franjo Majstor

197 Operations: The Center of Support and Control ........................... 2615
    Kevin Henry

198 Why Today’s Security Technologies Are So Inadequate: History, Implications, and New Approaches .......................... 2623
    Steven Hofmeyr

199 Operations Security and Controls ........................................... 2629
    Patricia A.P. Fisher

Section 9.2 Resource Protection Requirements

200 The Nebulous Zero Day .......................................................... 2641
    Robert M. Slade

201 Understanding Service Level Agreements ................................ 2645
    Gilbert Held

202 Physical Access Control ....................................................... 2651
    Dan M. Bowers

Section 9.3 Auditing

203 Auditing the Electronic Commerce Environment .......................... 2669
    Chris Hare

10 LAW, COMPLIANCE AND INVESTIGATIONS .................................. 2689

Section 10.1 Information Law ..................................................... 2693

204 Sarbanes-Oxley Compliance: A Technology Practitioner’s Guide .......... 2693
    Bonnie A.

205 Health Insurance Portability and Accountability Act Security Rule ....... 2697
    Lynda L. McGhie

206 Jurisdictional Issues in Global Transmissions ............................ 2701
    KbtmtiH
An Emerging Information Security Minimum Standard of Due Care

Robert Braun and Stan Stahl

ISPs and Accountability

Lee Imrey

The Case for Privacy

Michael J. Corby

Liability for Lax Computer Security in DDoS

Dorsey Morrow

Section 10.2 Investigations

Operational Forensics

Michael J. Corby

Computer Crime Investigation and Computer Forensics

Thomas Welch

What Happened?

Kelly J. Kuchta

Section 10.3 Major Categories of Computer Crime

Potential Cyber Terrorist Attacks

Chris Hare

The Evolution of the Sploit

Ed Skoudis

Computer Crime

Christopher A. Pilewski

Phishing: A New Twist to an Old Game

Stephen D. Fried

It's All About Power: Information Warfare Tactics by Terrorists, Activists, and Miscreants

Gerald L. Kovacich, Andy Jones, and Perry G. Luzwick

Section 10.4 Incident Handling

Social Engineering: The Human Factor in Information Assurance

Marcus K. Rogers

xxi
Privacy Breach Incident Response

Security Event Management

DCSA: A Practical Approach to Digital Crime Scene Analysis

What a Computer Security Professional Needs to Know about E-Discovery and Digital Forensics

How To Begin A Non-Liturgical Forensic Examination

Honeypot Essentials

Managing the Response to a Computer Security Incident

Cyber-Crime: Response, Investigation, and Prosecution

Glossary

Index