

# Information Security Management Handbook

introduction

Sixth Edition

\*

fcWntBll d ertnotni na , quoi^ eisnriH & loiter to JniTqmi ns ai ibediauA

\*

- @tipw ln3fnni9vo9 .2.U Uni^iio 03 mlsb oVI
- nfojq 35il-l)ijG no fiU^rTni lv;lnh^!

Section - >

haioop xi lsiifiti./n bU;::iiii-iJl ..^ojuoa bab-; \_^ •

'Jil bsnisJdo noiJutrrioini anisJiu)^ ilood airfT

vdi iolTO aUiiMsm lk

"olttaroid F Tiptbn, CISSP; Midki KraiiSevCisSEi

...^ajii' •!••• iibw alrfi flioi)-^lifishKxdsslff leiyjf8ni"3wi ifl^qo^oJodcf oi noiaainiraq-TOJ  
,EECio AJ/i ,«fi.^1 -JBJJ ,>w el i.ti;!•\* .••;VJ i; i |, .O3) .3nl .Istfi^D 9JTC1S313 liignvqoO sriJ iaeJno^io {\mc: fi^" •••• ^rww  
hgioiol .ai&iulo Ytahfvsiol noffrilaJgsi hnESSZIKDII eabivcnq Je/ll nobfixinigiujilaiq-ioVJofi eaid.^1 8VP

icft fino bwu sis birfl ,;

• IHHH6CHSCHULE  
^M ^ LIECHTENSTEIN

i [^3(M,noJqi'l -t bUnfiH \ jioodbci.ii BiWiothek luuciniuinl  
... 4s^ Q-v  
jtabnl bfls f»sn"

A Auerbach Publications , nI?cA\_P^n

A ^ j \ Taylor & Francis Group

• Stc>b-8 200

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

\_ ^ d s W ^ t b ^ n 9 4 w j « T 9 (tt feF/  
ro03,ni3OiiTtD«Bidly6J.www\\«itn

In ->Jif daW ibadi-iU A sill bus

# Table of Contents

ctl .

noiiBrmdiolio abiS ncmuH orH

Introduction.....•/.'\$vV;'i\*v:/AV;M,,,'.^v1;iw.^ ^ . . . . . xxiii

**Editors** —... —,.,.,.,..... ^..... 1. ^rai^BjRfiM\*(-jji4ioo\*s • • 44 — xxv

Contributors..... ^ . ? ? \* ..... xxvii

## 1 INFORMATION SECURITY AND RISK MANAGEMENT *it^z^M* m ^

### Section 1.1 Security Management Concepts and Principles

ion L Bits to Bytes to Boardroom ..... 9  
*Micki Krause*

2 Information Security Governance ..... 15  
*Todd Fitzgerald, ^ r^(io3 id) ^ninEd^):jrn9\$;nfiM rfoitRiwgftnoD HI*

3 Corporate Governance. . . . . 35  
*David C. Krehnke* ^ ' ' ^ TM^TV wcs \*a\*5«Kfi:.....

4 IT Governance Institute (ITGI) Overview.,,^u^aBO.BieQ•-£.t-••••• 45

5 Top Management Support Essential for Effective Information^ ^ Security. .... 51  
*Kenneth J. Knapp and Thomas E, MarshtM io ybotzu'J iam qiHsisnwO 01*

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

7 Information Security for Mergers and Acquisitions ..... 67  
**£M** ..... *Craig A. Schiller.* . . . . . :.v.. r-:(-...ri-; •> niity^i noiimmotal 1^

8 Information Security Governance ..... 89  
*Ralph Spert&r Poortfbo\* 3a3i ^nuJSt c gxtmubno.;*

Belts and Suspenders: Diversity in Information Technology Security. .... 95  
*Jeffrey Davis.* • • • • • ;'iv' • inmg'ji t iiiiujny^iivui/i XILUJJ-J\*.; ^ i i ' !

10	Building Management Commitment through Security Councils, or Security Council Critical Success Factors. . . . .	105
	<i>Todd Fitzgerald</i>	
11	Validating Your Business Partners. . . . .	123
— 12	Measuring ROI on Security. . . . .	133
	<i>Carl F. Endorf</i>	
13	The Human Side of Information Security. . . . .	139
	<i>Kevin Henry</i>	
14	Security Management. . . . .	155
	<i>Ken Buszta</i>	
15	It Is All about Control. . . . .	165
	<i>Chris Hare</i>	

## Section 1.2 Change Control Management

16	Patch Management 101: It Just Makes Good Sense! . . . . .	
	<i>Lynda L. McGhie</i>	
17	Security Patch Management: The Process. . . . .	185
	<i>Felicia M. Nicastro</i>	
18	Configuration Management: Charting the Course for the Organization. . . . .	201
	<i>Mollie E. Krehnke and David C. Krehnke</i>	

## Section 1.3 Data Classification

19	Information Classification: A Corporate Implementation Guide. . . . .	221
	<i>Jim Appleyard</i>	
20	Ownership and Custody of Data. . . . .	233
	<i>William Hugh Murray</i>	

## Section 1.4 Risk Management

21	Information Security Risk Assessment. . . . .	243
	<i>Samantha Thomas Cruz</i>	
22	Developing and Conducting a Security Test and Evaluation. . . . .	251
	<i>Sean M. Price</i>	
23	Enterprise Security Management Program. . . . .	261
	<i>George G. McBride</i>	

24	Technology Convergence and Security: A Simplified Risk/1 Management Model. . . . .	271
	<i>Km M. Shaurette</i>	
25	The Role of Information Security in the Enterprise Risk, 3 Management Structure. . . . .	281
	<i>Carl B. Jackson and Mark Carey</i>	
26	A Matter of Trusty 4>Hk>&> nk-mei\ vtAo'ikM ^-ihifixxi •naiHtfmokifc • • W-. . . . .	295
	<i>Ray Kaplan.</i>	
27	Trust Governance in a Web Services World. . . . .	311
	<i>Daniel D. Houser</i>	
28	Risk Management and Analysis. ^h3bi.0».^wM^Hrrf^m rri ri"-L*. . . . .	321
	<i>Kevin Henry</i>	
29	New Trends in Information Risk Management . . . . .	331
	<i>Brett Regan Young</i>	
30	Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security. . . . .	339
	<i>Carol A. Siegel, Ty R. Sagalow, and Paul SerriteUa</i>	

## Section 1.5 Policies, Standards, Procedures and Guidelines

31	Committee of Sponsoring Organizations (COSO) . . . . .	355
	<i>Mignona Cote</i>	
32	Toward Enforcing Security Policy: Encouraging Personal 'PfcififMttk. it*r for Corpoptate Information Security Policy. . . . .	367
	<i>J</i>	
33	The Security Policy Life Cycle: Functions and Responsibilities. . . . .	377
	<i>Patrick D. Howard</i>	
34	People, Processes, and Technology Combination. . . . .	389
	<i>Felicia M Nicastr&amp;&lt;i*^i^mi W^Q vlhu^aA MBIocpoO TI nc'to wsiiovO ^</i>	
35	Building an Effective Privacy Program. . . . .	401
	<i>Rebecca Herold</i>	
36	Establishing an E-Mail Retention Policy: Preventing Potential Legal Nightmares .. . . .	415
	<i>D. Fried</i>	
37	Ten Steps to Effective Web-Based Security Policif^il »«O ^««TT farlW OS Development and Distribution. . . . .	427
	<i>Fitzgerald</i>	

I*\S	38	Roles and Responsibilities of the Information Systems Security Officer. . . . .	443
		<i>Carl Burney</i>	
	39	Organizing for Success: Some Human Resources Issues in Information Security. . . . .	451
		<i>Jeffrey H. Fenton and James M. Wolfe</i>	
	40	Information Security Policies from the Ground Up. . . . .	465
		<i>Brian Shorten</i>	
H£	41	Policy Development. . . . .	475
		<i>Chris Hare</i>	
	42	Training Your Employees to Identify Potential Fraud and How to Encourage Them to Come Forward. . . . .	499
		<i>Rebecca Herold</i>	

## Section 1.6 Security Awareness Training

43	Change That Attitude: The ABCs of a Persuasive Security Awareness Program. . . . .	521
	<i>W. Chun</i>	
44	Maintaining Management's Commitment. . . . .	531
	<i>William Tompkins</i>	
45	Making Security Awareness Happen. . . . .	541
	<i>Susan D. Hansche</i>	
46	Beyond Information Security Awareness Training: It Is Time To Change the Culture. . . . .	555
	<i>Stan Stahl</i>	

## Section 1.7 Security Management Planning

47	Overview of an IT Corporate Security Organization. . . . .	567
	<i>Jeffrey Davis</i>	
48	Make Security Part of Your Company's DNA. . . . .	579
	<i>Ken M. Shaurette</i>	
49	Building an Effective and Winning Security Team. . . . .	591
	<i>Lynda L McGhie</i>	
50	When Trust Goes Beyond the Work Offshore. . . . .	607
	<i>Stephen D. Fried</i>	

51	Maintaining Information Security during Downsizing . . . . .	19
	<i>Thomas J. Bray</i>	
52	The Business Case for Information Security: Selling Management on the Protection of Vital Secrets and Products' . . . . .	625
	<i>Sanford Sherizen</i>	
53	How to Work with a Managed Security Service Provider. . . . .	631
	<i>Laurie Hill McQuillan</i>	
54	Considerations for Outsourcing Security . . . . .	643
55	The Ethical and Legal Concerns of Spyware . . . . .	
	<i>Eric C. Sipior, Bruce T Ward, and Georgina R. Roselli</i>	

## Section 1.8 Ethics . . . . .

56	Ethics and the Internet . . . . .	673
	<i>Micki Krause</i>	
57	Computer <i>Peter S. Tippett</i> , <i>Y</i>	

## Section 2.1 Access Control Techniques ; . t ' . . . . .

58	A Look at RFID Security. . . . .	
	<i>Ben Rothke</i>	<b>HJBWA lo aborfM 5.1</b>
59	New Emerging Information Security Technologies and Solutions , »   i " . . . . .	
	<i>Tara Chand</i>	
60	Sensitive or Critical Data Access Control . . . . .	739
	<i>Mollie E. Krehnke and David C Krehnke</i>	
61	An Introduction to Role-Based Access Control . . . . .	751
	<i>Ian Clark</i>	
62	Smart Cards. . . . .	765
	<i>James S. Tiller</i>	
63	A Guide to Evaluating Tokens. . . . .	775
	<i>Joseph T. Hootman</i>	<b>"•&amp; ^ne \$nnoJinoM dS noiis?</b>
64	Controlling FTP: Providing Secured Data Transfers . . . . .	785
	<i>Chris Hare</i>	

## Section 2.2 Access Control Administration

\*M ie

- 65 End Node Security and Network Access Management: Deciding  
Among Different Strategies.....T...\*,..... 803  
£M..... ^hrsH ofJ no  
*Franjo Majster* .. , - . -  
, 66 Identity Management: Benefits and Challenges, ....., - .., # f.. w. . . . 823  
?I I. McGrtie
- 67 Blended Threat Analysis: Passwords and Policy, \*>., \*..... , \*,, \*!\*.\*«.«.»- . . . . 843  
*Darnel D. Houser*

## 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* . i-ni <t .1 »rli bnfi 2jiril3 d^

## Section 2.4 Access Control Methodologies and Implementation

- 70 Centralized Authentication Services (RADIUS, TACACS,  
DIAMETER)..... 90?  
*Bilistackpole* \_ JQHTVTO3 ^^
- 71 An Introduction to Secure Remote Access,.....^ ..... 92;  
*JVI. DHC\**

## Section 2.5 Methods of Attack

- ^0" 72 Hacker Tools and Techniques ', JfffWW?. WtWCO'iohiJaWSPCJA y«W.. PA. . . . 935  
£\* SJtoudu hmuO
- 73 A New Breed of Hacker Tools and Defenses.....MiO. W.TftiftQ&.. PA. . . . 951  
Ed SJtowfc
- 74 Hacker Attacks and Defend 2 .<¥»>pAJ^Kt9.-?IvA A^ RQJ^H^ojjnl.nA.. JA. . . . 965  
*Ed Skoudis* \*u\*D nul
- 75 Counter-Economic Espionage. ....>i..i.\*itefJ?J?R&M. . . . 977  
*Craig A. Schiller* . v!:W. ;• Mxin\

## Section 2.6 Monitoring and Penetration Testing

ol obkfo A €I

- 76 Insight into Intrusion Prevention System\*liiwwfl;.KT3. SAilUrtVloU.. M. . . . 993  
*Deograt-Lumy and Roy Naldo*





## 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*

101	Closed, c; i » a f t ; ® ( ^ <i>David Antzau</i>	ngieaCI bra* ti
-----	---	--------------------

**Section 4.2 Technical Controls**      ••\$ nomnwo

102	Types of Information Security Controls.....	1357
	<i>Harold F. Tipton</i>	

**Section 4.3 Environment a**

103	Workplace Violence: Event Characteristics* <sup>13no^</sup> ZWnfcufl I-d and Prevention.....	1367
••'-•	<i>George Richards</i>	
104	Physical Security: The Threat after September 11, 2001.....	1373
—	<i>Jaymes Williams</i>	

**5 SECURITY ARCHITECTURE AND DESIGN** .,4<sub>to</sub>M..gj.i. 1393

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

v , j	105 <u>Enterprise Assurance: A Framework Explored, !..</u> .....	1397
	<i>Bonnie A. Goins</i>	
	106 <u>Creating a Secure Architecture m j,*f r&amp;h'O &amp;JM2</u> .....	1403
	<i>Christopher A. Pilewski and Bonnie A. Goins</i>	
	107 <u>Common Models, for Architecting an Enterprise Security, - r , , —</u> .....	17^9
	<i>CsDclullitV</i>	1413
	<i>Matthew J. Decker'</i>	
	108 <u>The Reality of Virtual Computing</u> .....	1431
	<i>Chris Hare</i>	

**Section 5.2 Principles of Security Models, Architectures and Evaluation Criteria**

109	Formulating all Enterprise Informatidfi-ii<89aKA]3i;qrnU33ni2ua9HT IZI Security Architecture v-lwakAWwWQfftM^WM^WnJmQ^OKV.ll <sup>1</sup> .....	1451
	<i>Mollie E. Krehnke and David C. Krehnke</i>	
110	Security Architecture and Models .\\b\K&VI&Vf&. &>WIW&\$ptiii\$£.,.£ti... 1469	
	<i>Foster J. Henderson and Kellina M. Craig-Henderson</i>	
111	The Common Criteria for IT Security Evaluation irtqaruXuatUioittS.. AS j . . . 1487	
	<i>Debra S. Herrmann</i>	

## Section 5.3 Common Flaws and Security Issues: System Architecture and Design

- 112 Common System Design Flaws and Security Issues ...;Uul33>T\*  
*William Hugh Murray*

## 6 BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY PLANNING

### Section 6.1 Business Continuity Plajining ^v.r/ KiWfrnn mr

- 113 Developing Realistic Continuity Planning Process Metrics Jifitt\* wt<S\*P\* .....1515  
*Carl B. Jackson*
- 114 Building Maintenance Processes for Business Continuity Plans. ....1529  
*Ken Doughty*
- 115 Identifying Critical Business Functions ..- J.3Xro3fIL &.OJUIU332 1541  
*Bonnie A. Goins*
- 116 Selecting the Right Business Continuity Strategy.,  
*Ken Doughty*
- 117 Contingency Planning Best Practices and Program Maturity. ....";\_\_\_\_1557  
*Timothy R. Stacey*
- 118 Reengineering the Business Continuity Planning Process...?'?...,\*, ..... 1579  
*Cart a. fackson*
- 119 The Role of Continuity Planning in the Enterprise Risk Management Structure. ....;.....- ..... 1587  
*Carl B. Jackson*

itfrl .. ' i>I wfl' 801

### Section 6.2 Disaster Recovery Planning

- 120 Contingency at a Glance ^M T^."???.??.??.?  
*Ken M. Shaurette and Thomas J. Schleppenbach* ; . " i3 noitSIil
- 121 The Business Impact Assessment Process and the Importance of Using Business Process Mapping ..... 4tW\*\*i»MH\*.i(\*i«tt»a."«"\*\*\*  
*Car/ B. /acfeson* vAwrt-.\*^ 3 |iivaC\ tom sjlnAvOL 3 St
- 122 Testing Business Continuity and Disaster Recovery Plans ..^tii^u...^ . . . . 1629  
*James S. Mitts* nomiamH -ymO M nniihA tonn noi-nbmH .1
- 123 Restoration Component of Business Continuity Planning...itaoD-adT.-.t . . . 1645  
*John Dorfand Martin Johnson* nntunroH Z

- 124 Business Resumption Planning and Disaster Recovery. A Case History. . . . .1655  
*Kevin Henry*
- 125 Business Continuity Planning: A Collaborative Approaches. . . . .1665  
*Kevin Henry*

**Section 6.3 Elements of Business Continuity Planning**

- 126 The Business . . . . .1675  
*Car/ B. Jackson*

**7 TELECOMMUNICATIONS AND NETWORK SECURITY . . . . .1693**

**Section 7.1 Communications and Network Security**

- 127 Network Security Utilizing an Adaptable Protocol FrameworkaGV0t3\* • \*H1 • • •  
*Robby Fussell*
- 128 The Five W's and Designing a Secure, Identity-Based, Self-Defending Network  
*Samuel W. Chun*
- 129 Maintaining Network Security: Availability via Intelligent Agents . . . . .1721  
*Robby Fussell*
- 130 PBXFirewalls: Closing the Back D r i d r ^ ^ A ' ? ^ ? . ^ . . . . 1731  
*William A. Yarberr, Jr.*
- 131 Network Security Overview. . . . . ^ ^ TMT?T^Y.. ^J.'... 1739  
*Bonnie A. Goins and Christopher A. Pilewski*
- 132 Putting Security in the Transport: TLS . . . . . 1751  
*Chris Hare*
- 133 WLAN Security Update. . . . .ft#3 A?\* ??!<#!.^HX1^.^AW??...^i... 1761  
*Franjo Majstor*
- 134 Understanding SSL . . . . ^ v u v r v V v v . v v v ^ ^ ^ . ^ ^ ^ ^ ^ Y . ^ S . . . Of!... 1777  
*Chris Hare*
- 135 Packet Sniffers and Network M o i u t ^ . ^ t a ^ ^ . V C V ? ^ ^ ^ ^ \* " \_ ^ 1 \_ \_ \_ 1791  
*S. Ti/ter and Bryan D. Fish ibhW&J -3*
- 136 Secured Connections to External Networlik<;W^^«M-.«Pfe'Jau4.ACJ... 1811  
*Steven F. Blanding*
- 137 Security and Network Technologies .-&«fe/kl ,T^SI3Wflifl»#twUtaj&, ..^J... 1827  
*Chris Hare*

138	Wired and Wireless Physical Layer Security Issues <i>James Trulove</i>	1847
139	Network Router Security <i>Steven F. Blanding</i>	1855
140	What's Not So Simple about SNMP? <i>Chris Han</i>	1867
<b>6</b>		
141	New Work and Telecommu Ground Up <i>Matthew J. Decker</i>	1879
<b>Section 7.2</b>	<b>Internet, Intranet, Extranet Security</b>	
142	Security and the Physical Network <i>Matthew J. Decker</i>	
143		
144	ISO/OSI and TCP/IP Network Model Characteristics <i>George G. McBride</i>	1917
<b>Section 7.2</b>	<b>Internet, Intranet, Extranet Security</b>	
145	VoIP Security Issues <i>Anthony Bruno</i>	1929
146	An Examination of Firewall Architectures <i>I. Heory</i>	1941
147	Voice over WLAN <i>Bill Lipiczky</i>	1997
148	Spam Wars: How To Deal with Junk E-Mail <i>Al Bredenberg</i>	2007
149	Secure Web Services: Holes and Fillers <i>Lynda L McGhie</i>	
150	IPSec Virtual Private Networks <i>James S. Tiller</i>	
151	Internet Security: Securing the Perinete/ <i>Doug/as G. Conorch</i>	2051
152	Application-Layer Security Protocols for <i>Bi/; Stackpole</i>	
153	Application Layer: Next Level <i>Keith Pasley</i>	



168	Packet Sniffers: Use and Misuse	2243
	<i>Steve A. Rodgers</i>	
169	ISPs and Denial-of-Service Attacks	2253
	<i>K. Narayanaswamy</i>	

## 8 APPLICATION SECURITY 2263

### Section 8.1 Application Issues

170	Application Service Provider Security: Ensuring a Secure Relationship for the Client and the ASP	2267
	<i>Stephen D. Fried</i>	
171	Stack-Based Buffer Overflows	2289
	<i>Jonathan S. Held</i>	
172	Web Application Security	2301
	<i>MandyAndress</i>	
173	Security for XML and Other Metadata Languages	2311
	<i>William Hugh Murray</i>	
174	XML and Information Security	2319
	<i>Samuel C. McClintock</i>	
175	Application Security	2327
	<i>Walter S. Kobus, Jr.</i>	
176	Covert Channels	2335
	<i>Anton Chuvakin</i>	
177	Security as a Value Enhancer in Application Systems Development	2343
	<i>Lowell Bruce McCulley</i>	
178	Open Source versus Closed Source	2361
	<i>£(i Skoudis</i>	
179	A Look at Java Security	2381
	<i>Ben Rothke</i>	

### Section 8.2 Databases and Data Warehousing

180	Reflections on Database Integrity	2387
	<i>William Hugh Murray</i>	
181	Digital Signatures in Relational Database Applications	2395
	<i>Mike R. Prevost</i>	

- 182 Security and Privacy for Data Warehouses: Opportunity, or TJuelfcM.. 261... 2405  
*David Bonewell, Karen Gibbs, and Adriaan Veldhuisen*

## Section 8.3 Systems Development Controls ...<sup>a</sup> ,,

- ^3 Building and Assessing Security, in the Software Development, Lifecycle.....\*{<<<4&Wf&:?. 2425  
*George G. McBride*  
;• i,. ifiup^bKnl oP nA zargolonrbsT ifihioaS e^aboT yriW 8^t
- !8<sup>4</sup> Avoiding Buffer Overflow Attacks^,&fr<sub>1</sub>#w^w!#%kti&••&&\$&\$&&:. 2437  
*Sean M. Price*
- 185 Secure Development Life Cycle .... ^oMflos'bos ^JIBM& emii<finqO' • •\*«\*• • • 2449  
*Kevin Henry*
- 186 System Development Security Methodology..... 2457  
*Ian Lim and Ioana V. Bazavan*
- 187 Software Engineering Institute Capability Maturity Model..... 2475  
*Matt Nelson* .. • ..... ilolnibM «\*!'• • -0tif
- 188 Enterprise Security Architecture..... 2491  
?! \*.. ' . *William Hugh Murray* ^nvm^A bvs.I.»ivi3<i gnbafijzisbnJJ. .10S.
- 189 Certification and Accreditation Methodology..... 2503  
£. i&e^Hte ami *David C. Krehnke* • ><noD 3833^A luaigyri^ SOI
- 190 System Development Security Methodology..... 2521  
*Ian Lim and Ioana V. Bazavan*
- 191 Methods of Auditing Applications..... f..... 2521  
*David C. Rice and Graham Bucholz*

snbibuA ZM

## Section 8.4 Methods of Attack

- 192 Hackin<sub>s</sub> Mejhod^ ^T^ffv^i-HlVtA \*3!>MAIOTMOO';W^:J" • 2547  
*Georges J. Jahchan*
- 193 Enabling Safer Deployment of Internet Mobile Code o'ifll I.Of Technologies .....^..... 2557  
*Ron Moritz* ^-. T O i f e ^ j ^ ^ MI

## 9 OPERATIONS SECURITY.....; " ^ . » . ^ ..... 2569

### Section 9.1 Concepts

- 194 Security Considerations in Distributed Computing: A Grid Security Overview .. ..\nM9i¥)Vi^A.W^j¥^i4i^M£?i\<&M^!9IU^Hmi^L -. A^i... 2573  
*Sasan Hamidi* swtfl-noiaaqE



195	Managing Unmanaged Systems .....	2579
	<i>Bill Stackpole and Man Nguyen</i>	
196	Storage Area Networks Security Protocols and Mechanisms .....	2597
	<i>Franjo Majstor</i>	
197	Operations: The Center of Support and Control: ?..!': .....	2615
	<i>Kevin Henry</i>	
198	Why Today's Security Technologies Are So Inadequate: History, Implications, and New Approaches. ....	2623
	<i>Steven Hofmeyr</i>	
199	Operations Security and Controls. ....	2629
	<i>Patricia A.P. Fisher</i>	

## Section 9.2 Resource Protection Requirements

200	The Nebulous Zero Day. ....	2641
	<i>Robert M. Slade</i>	
201	Understanding Service Level Agreements. ....	2645
	<i>Gilbert Held</i>	
202	Physical Access Control. ....	2651
	<i>Dan M. Bowers</i>	

## Section 9.3 Auditing

203	Auditing the Electronic Commerce Environment. ....	2669
	<i>Chris Hare</i>	

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

## Section 10.1 Information Law .i\_n(, triim ^i^o i^£? sniMr,r'

204	Sarbanes-Oxley Compliance: A Technology Practitioner's Guide. ....	2693
	<i>Bonnie A.</i>	
205	Health Insurance Portability and Accountability Act Security Rule. ....	2700
	<i>Lynda L. McGhie</i>	
206	Jurisdictional Issues in Global Transmissions. ....	2700
	<i>encer Poor^</i>	

207	An Emerging Information Security Minimum Standard of Due Care. . . . .	2725
	<i>Robert Braun and Stan Stahl</i>	
208	ISPs and Accountability. . . . .	2745
	<i>Lee Imrey</i>	
209	The Case for Privacy — . . . . .	2761
	<i>Michael J. Corby</i>	
210	Liability for Lax Computer Security in . . . . .	2767
	<i>Dorsey Morrow</i>	

## Section 10.2 Investigations

211	Operational Forensics. . . . .	2773
	<i>Michael J. Corby</i>	
212	Computer Crime Investigation and Computer Forensics. . . . .	2781
	<i>Thomas Welch</i>	
213	What Happened?. . . . .	2813
	<i>Kelly J. Kuchta</i>	

## Section 10.3 Major Categories of Computer Crime

214	Potential Cyber Terrorist Attacks. . . . .	2817
	<i>Chris Hare</i>	
215	The Evolution of the Sploit. . . . .	2831
	<i>Ed Skoudis</i>	
216	Computer Crime. . . . .	2845
	<i>Christopher A. Pilewski</i>	
217	Phishing: A New Twist to an Old Game. . . . .	2853
	<i>Stephen D. Fried</i>	
218	It's All About PowenInformation Warfare Tactics by Terrorists, Activists, and Miscreants. . . . .	2873
	<i>Gerald L. Kovacich, Andy Jones, and Perry G. Luzwick</i>	

## Section 10.4 Incident Handling

219	Social Engineering: The Human Factor in Information Assurance. . . . .	
	<i>Marcus K. Rogers</i>	<i>and hacking</i>

220	Privacy Breach Incident Response. ;^u»^i wuw«iUj^jlgii^a.ft/t!ii^&.*^..Oi... 2911 <i>Rebecca Herold</i> . . . . .	
221	Security Event Management . . . . . i«-u* w,,*~.^-,,,,*,;*,,,,-. 2929 <i>Glenn Cater</i> . . . . . -..U-.TTJA brus/-I2I 8ff£	
222	DCSA: A Practical Approach to Digital Crime Scene Analysis. . . . . •**'/«« «* »RI£><M{T. • *90£. • • 2945 <i>Marcus K. Rogers</i> . . . . . Au->j i'-.;.;,;.	
223	What a Computer Security Professional Needs to Know ab.QUt/jjfoErJ . . •{\$£. . . • E-Discovery and Digital Forensics. . . . . wmtAA-^ViiU. . . . . 2961 <i>Larry R. Leibrock</i> . . . . . **	
224	How To Begin A Non-Liturgical Forensic , ntoitfigil297nl 1.01 noitD^g Examination . . . . . ,,,, ,,,, ,,,, . 2967 <i>Carol Stucki</i> . . . . . ,*;&,,.«, & l(nnii,,n i" , ; i'	
225	Honeypot Essentials . . . . . 2983 <i>Anton Chuvakw</i> ^..^ 19ilKimor> f)ff£ n.^h-'ivnl smnDtTOftjn'nn'i • i'f.	
226	Managing the Response to a Computer Security ' Incident . . . . . <i>Michael Vangelos</i>	
227	Cyber-Crime: Response, Investigation, and Prosecution. . . . . nr«o!)'tl <i>Thomas Akin</i>	
228	Glossary ..... V^?. 1/; ^/l&.FJV/X: 1:?. *:?}.. A! /... 3009	
229	Index . . . . . ^ v . v . . . . . 3151 if<^r . . . . . "in"J -'I' to nortuiovHaril -fs.	

.D '{Twft tuta

indbbal ^.01

iictmoinl nt lOfjeH nmmnH orfT :^nn