
INDEX

A

Absolute Software Corporation, 202
AccessData Corporation, 202
Acronyms, 231
ActivCard, Inc., 202
Aladdin Knowledge Systems, Inc., 202
Alternative Computer Technology, Inc., 202
Amazon.com, 28–29
American Society for Industrial Security (ASIS), 191
Archibald, Matthew, 123
ArcSight, 203
Argus Systems Group, Inc., 203
Astaro Corporation, 203
@Stake, 195
Attacks, *See also* Break-ins
 background checks, 14–15
 and clear-cut responsibilities, 14
 Computer Security Incident Response Team (CSIRT), 14
 containing, 13
 documenting, 14
 escalation of the problem, 15
 follow-up, 16
 game plan, following, 15
 incident-response nightmare, 3–8
 incident-response procedures, training in, 13
 Incident-Response Team (IRT), 12
 intruder, identifying, 14
 Intrusion-Detection Systems (IDSs), 11
 likelihood of experiencing, 9–10
 Point of Contact (POC), designating, 13
 prevention, 8–9

 recognizing, 11
 and recordkeeping, 15
 responding to, 3–20
 and security budget, 16
 senior management, notifying, 13, 16
 system snapshot, 14
 trust, 14–15
 understanding/prioritizing, 13–15
Audit logs, 107
Audits, 61–63
 conducting, 108
Authenex, 203
Authenticate, 203
Aventail Corporation, 203

B

Bace, Rebecca, 83
Baltimore Technologies, 203–4
Bigfix, 204
Bindview Development, 204
Biometric Access Corporation, 204
BLOCKADE Systems Corporation, 204
BLUE LANCE, 204
BorderWareTechnologies Inc., 205
Breach of contract suits, 149
Break-in reports, 14
Break-ins, *See also* Attacks
 checklist, 16–17
 quick response to, 108
 written policy for dealing with, 13–14
BRICKServer, 205
Buddy System, The, 205
Budget:
 adding encryption to, 114
 and attacks, 16
 for security training, protecting, 79
Bugs, 65

- Bugtraq, 195
- “Bullet” approach to security, 16
- Buy.com, 28–29
- C**
- Camelot, 205
- Captus Networks, 205
- CERIAS, 192
- CERT Coordination Center (Carnegie Mellon University), 29, 33, 191
- Certco, 205
- Certicom Corporation, 205–6
- Cgichk, 198
- Chambersburg Museum of Art case study, 114–19
 - as casualty of war, 118–19
 - corporate network, bypassing, 114
 - evidence collection, 115–16
 - security:
 - ownership of, 117–18
 - transferring responsibility for, 118
 - system administrator vs. security team, 116–17
- Check Point, 206
- Checklist:
 - break-ins, 16–17
 - executive support, 49–50
 - internal network security, 121
 - network access, 66
 - outsourcing, 133–34
 - risk, 32–33
 - roles/responsibilities, 109
 - training, 81–82
 - unplanned security, 95
- Chief Information Officer (CIO), 13
- Chrysalis-ITS, 206
- C.I. Host* case, 148, 150–51
- Cigna Insurance, 197
- Cisco Systems, Inc., 206
- Citadel Computer Systems, 206
- CloudNine Communications, 110
- CMS Technologies, 206
- Code Red/Code Red II, 11, 67
- Codex Data Systems, 206–7
- Cogentric, 207
- Communication Devices, Inc., 207
- Computer Associates, 207
- Computer Incident Advisory Capability (CIAC), 192
- Computer Oracle and Password System (COPS), 198
- Computer Sciences Corporation, 207
- Computer Security Incident Response Team (CSIRT), 14
- Computer Security Institute (CSI), 10, 192
- Computer Security Products, Inc., 208
- Computer Sentry Software, 207
- ComputerCOP Corporation, 207–8
- Configuration errors, with network services, 65
- Conflict-of-interest escalation, 14
- Conclusive, 208
- CONSUL risk, 208
- Consulting firms, 195–96
- COPS, 198
- Coroner’s Toolkit, 198
- Costa Corp case study, 145–54
- Counterpane Internet Security, Inc., 208
- Crack program, 31, 41–42, 198
- Cranite Systems, 208
- Cross-organizational security support, delineating, 119–20
- CRYTOCard, 208–9
- Customer information, protecting, 13
- CVE, 194
- Cyber Safe Corporation, 209

Cyber-Ark Software, 209
 CyberGuard Corporation, 209
 Cyber-jihad, 159
 CyberSafe, 214
 Cyber-SIGN, 209
 CyberSoft, Inc., 209
 Cylink, 209–10

D

Data Systems Analysts, 195
 Datacard Corporation, 210
 DataKey, Inc., 210
 DataLynx, Inc., 210
 de Raadt, Theo, 19
 Deloitte Touche & Tohmatsu, 195
 Denial-of-service attacks, 65
 Department of Defense (DOD), 17–18
 Department of Justice (DOJ), 197
 Detection software, 11, 107
 Digital Delivery Inc., 210
 Disgruntled employees, as fugitive hackers, 158
 Dittrich, David, 30
 DIVERSINET Corporation, 210
 Documenting an attack, 14
 Doktor Nuker, 159
 Dormant user accounts, 30
 Dsniff, 199

E

eBay, 28–29
 eEye Digital Security, 211
 Electronic Frontier Foundation (EFF), 192
 Email hazards, 141–42
 Encrypted email, 138–41
 ENSURE Technologies, 210–11
 Entegrity Solutions, 211

Entercept SecurityTechnologies, 211
 Entrust Technologies, 211
 Ernst &Young LLP, 196
 eSecurity, Inc., 211
 eSecurityOnline LLC, 212
 esniff, 6
 Executive management, reporting back, 46–47
 Executive security summary, 47–48
 Executive support, 37–51
 commitment, 38–44
 security break-ins, 40–43
 unsecured systems, 39–40
Exigent case, 148, 150
 External connections:
 requiring approval for, 64–65
 tracking, 63–64
 External escalation, 14
 EyeDentify, Inc., 211

F

Farmer, Dan, 18, 69, 107
 Federal Bureau of Investigation (FBI), 197
 File permissions, exporting, 30
 FinJan, 212
 Firewall, 199
 Firewalls:
 audit logs, 107
 audits, conducting, 108
 break-ins, quick response to, 108
 detection software, 107
 feeding, 107
 getting educated about, 108–9
 Global Chips case study, 102–4
 list, 195
 policies/procedures, developing, 106
 proof of security, requiring, 108

- FIRST, 192
- First Fidelity case study, 3–8
- First-strike attacks, 11
- FishNet Consulting, Inc., 196
- Forensic Challenge, 29–30
- Forescout, 212
- Foundstone, 212
- F-Secure Inc., 212
- Fugitive hackers, 158–59
 - disgruntled employees, 158
 - hacktivists, 159
 - industrial spies, 158–59
 - lone sociopaths, 159
- Funk Software, Inc., 212
- G**
- Game plan, following, 15
- Garfinkle, Simson, 97–110
- Gemini Computers, Inc., 213
- Gemplus Corp, 212–13
- G-Force, 159
- Gilian Technologies Inc., 213
- Global Chips case study, 100–107
 - firewall, 102–4
 - firewall administrator, 101–4
 - internal attitudes, 104–5
 - management and security, 102–3
- Global Technologies Group, Inc., 213
- Global Technology Associates, Inc., 213
- GNUPG, 199
- Gramm-Leach-Bliley Act (GLBA), 149–50, 154
- Great Circle Associates, 213
- Guardent, 196
- Guidance Software, 213–14
- H**
- Hacker theft, organized nature of, 27
- Hacker tools, 159
- Hackers, xxii, 157–90
 - fugitive hackers, 158–59
 - profile, 158–60
 - reformed, 12
 - reports of break-ins, 40
 - tools, 159–60
 - walking with, 160–89
- Hactivists, 159
- Hager, Mike, 35
- Harris Corporation, 214
- Hewlett-Packard Corporation, 214
- Hifn, 214
- High Technology Crimes Investigation Association (HTCIA), 192
- HIPPA (Health Insurance Portability and Accountability), 149, 154
- Honey Project, 29–30
- Hping2, 199
- I**
- IBM, 214
- ICSA, 193
- Incident-response nightmare, 3–8
 - hacker, 6–7
 - incident escalation, 6
 - inside attacks, 7–8
 - problem fix, 4–5
 - security breach, 5–6
 - unauthorized access, 5
- Incident-response procedures, training, 13
- Incident-Response Team (IRT), 12
- Industrial spies, 158–59
- Info Express, Inc., 214
- Info Security News, 194
- Information assets, fiduciary responsibility to protect, 151–52

- Information Systems Security Association (ISSA), 193
 - Information technology, insuring, 197–98
 - Information Warfare: Chaos on the Information Superhighway* (Schwartz), 63
 - Inside attacks, 7–8
 - Integralis, 215
 - Intel Corporation, 215
 - Intellitactics.com, 215
 - Intermint Financial case study, 72–78
 - fact gathering, 73–74
 - security training, 76–77
 - funding for, 78
 - system testing, 74–76
 - Internal escalation, 14
 - Internal network security, 113–22
 - Chambersburg Museum of Art case study, 114–19
 - checklist, 121
 - cross-organizational security support, delineating, 119–20
 - policies/procedures, responsibility for, 119
 - processes, questioning, 120
 - and system administrator, 121
 - Internet abuse, 64
 - Internet Firewalls FAQ, 105–6
 - Internet Society, 193
 - Intruder, identifying, 14
 - Intrusion Inc., 215
 - Intrusion-Detection Systems (IDSs), 11
 - IntruVert, 215
 - Investigative Group International, 215
 - IP Filter, 199
 - ISC² (International Information Systems Security Certification Consortium), 193
 - ISO 17799, 154
 - ISP/client relationship, 26
- J**
- JFC Pharmaceutical case study, 56–63
 - hacker, 57
 - network maps, 58–59
 - risk list, 61
 - security architecture, 56
 - security audits, 61–63
 - security installation policy, 56–57
 - taking responsibility for security, 61–62
 - unenforced policies, 59–60
 - unscheduled security test, 57–58
- K**
- Kirby, John, 143
 - Klaxon & Tocson, 199
 - Kroll, 196
 - Kyberpass Corporation, 216
- L**
- L0phtCrack, 199
 - Lancope, 216
 - Langin, Dan J., 147, 152
 - LJK Software, 216
 - Lloyd's, 198
 - Lone sociopaths, as fugitive hackers, 159
 - Lsof, 199
 - Lucent Technologies, 216
 - Lumeta Corporation, 216
- M**
- Maintaining security, 97–110
 - Global Chips case study, 100–106
 - Malicious code outbreaks, 141–42
 - Malicious hackers, 10
 - Management:
 - communicating to, 49
 - notifying of attacks, 13, 16

- reporting back to, 46–47
- and security, 49
- security checklist, 49–50
- training, 79
- McAfee, 216
- McConnell's Drugs case study, 56–63
 - competition, 62–63
 - hacker, 57
 - JFC Pharmaceutical, 56–65
 - network maps, 58–59
 - security architecture, 56
 - security installation policy, 56–57
 - unenforced policies, 59–61
 - unscheduled security test, 57–58
- MessageLabs, 216
- N**
- National Infrastructure Protection Center (NIPC), 51, 193
- nCipher Corporation Ltd., 216
- nCircle, 217
- Nessus, 200
- NetDynamics, 137
- Netegrity, Inc., 217
- netForensics, 217, 218
- NetIQ Corporation—WebTrends Corp., 218
- NetScreen Technologies, Inc., 217
- Network Associates, 217–18
- Network Defense, 196
- Network Engineering Software, Inc., 218
- Networks, 55–67
 - checklist, 66
 - external connections:
 - requiring approval for, 64–65
 - tracking, 63–64
 - follow-up, 66
 - JFC Pharmaceutical case study, 56–63
 - McConnell's Drugs case study, 56–63
 - policies/procedures, enforcing, 65
 - standard architecture designs, using, 63
 - system administrator responsibilities, 64–65
 - training, stressing the importance of, 65
 - unnecessary services, disabling, 65
 - unsecured systems, connecting to the Internet, 66
- Network-1 Security Solutions, Inc., 217
- NFR Security, 218
- NIKSUN Inc., 218
- Nimda, 11
- Nokia Internet Communications, 219
- NPASSWD, 200
- NT Bugtraq, 195
- O**
- Office of Homeland Security, 194
- Old accounts, removing, 30
- OmniSecure, 219
- OneSecure, 219
- OpenSSH, 200
- OPIE, 200, 202
- Out-of-the-box security, 21–33
 - assigning/acquiring funding for, 29–30
 - network testing, 28
 - out-of-the-box system installations,
 - avoiding, 28
 - risks, recognizing, 27
 - systems experts, familiarizing yourself with, 28–29
- Out-of-the-box system installations,
 - avoiding, 24, 28, 56–57
- Outside experts, working, 31–32
- Outsourcing security, 125–34

- checklist, 133–34
- fixing problems, 132
- planning, 92
- S&B Systems case study, 126–31
- security assessments, conducting, 132
- sink-or-swim approach to security, 133

P

- Palisade Systems, 219
- PassLogix, 219
- Passwords, testing, 30–31
- Pelican Security, 219
- PentaSafe Security Technologies, Inc., 219–20
- Phaos Technology Corporation, 220
- Point of Contact (POC), designating, 13
- Policies/procedures:
 - developing for firewalls, 106
 - enforcing, 65
 - following, 31
 - responsibility for, 119
- PostX Corporation, 220
- Predictive Systems, Inc., 196, 220
- Prevention, 8–9
 - unforeseen problems, 11
- PriceWaterhouseCoopers, 196
- Product vendors, 202–30
- Promptus, 220
- Proof of security, requiring, 108
- Protegrity, 220
- Psionic Technologies, 220

Q

- Qualys, Inc., 221

R

- Rainbow Technologies, 221
- Ranum, Marcus, 16, 105–6, 108, 155
- Read/write permissions, exporting, 30

- Recognition Systems Inc., 221
- Recordkeeping, and attacks, 15
- Recourse Technologies, 221
- Report protocols, 16
- Riptech (Symantec), 221
- Risk, checklist, 32–33
- Risks, recognizing, 27
- RiskWatch, 221
- Rockland General case study, 86–92
 - outsourcing, planning, 92
 - personal information at risk, 91–92
 - physical controls, getting past, 88–89
 - physical security, 88
 - risk, understanding, 88
 - security testing, 87–88
 - unauthorized access, 89–90
- RockSoft, 221
- RSA Data Security, 222

S

- S&B Systems case study, 126–31
 - Express Time, 126–28, 131
 - management, 131
 - network connections, 127–28
 - security controls, 126–27
 - security mistakes, 129–30
 - support, 130–31
- S⁴Software, Inc., 222
- Safetynet Security, 222
- SAGE, 194
- SAIC (Science Applications International Corporation), 107, 196, 222
- SAINT Corporation, 222
- Sandstorm Enterprises, Inc., 222
- SANS Institute, 80, 193
- SATAN (System Administrator's Tool for Analyzing Networks), 107, 200
- Savvydata, 222

- Schlumberger, 223
- Schultz, Gene, 1
- Schwartau, Winn, 63
- SEARCH, 194
- Secure Computing, 223
- SecureLogix Corporation, 223
- SecureNet Technologies, 223
- SecureWorks, 223
- Securify, Inc., 196, 223
- Security:
 - assigning/acquiring funding for, 29–30
 - audit logs, 107
 - audits, conducting, 108
 - break-ins, quick response to, 108
 - budget, 16
 - adding encryption to, 141
 - committing to, 44–45
 - crime investigation, 196–97
 - delegation of, 45
 - executive management, reporting back to, 46–47
 - executive support, 37–51
 - firewall policies/procedures, developing, 106
 - firewalls, feeding, 107
 - firewalls, getting educated about, 108–9
 - future of, 145–54
 - internal network security, 113–22
 - mailing lists, 195
 - maintaining, *See* Maintaining security and management, 49
 - management levels involved in, keeping to a minimum, 45–46
 - network access, 55–67
 - old accounts, removing, 30
 - out-of-the-box, 21–33
 - outside experts, working with, 31–32
 - outsourcing, 125–34
 - passwords, testing, 30–31
 - patches, applying, 31
 - policies/procedures, following, 31
 - proof of security, requiring, 108
 - read/write permissions, exporting, 30
 - resources, 194
 - roles/responsibilities:
 - checklist, 109
 - defining, 106
 - setting as a corporate goal, 48
 - software, 198–202
 - training, 32, 71–82
 - training programs, providing, 49
 - unplanned, *See* Unplanned security
 - unsecured email, 137–42
 - vulnerability archives, 194–95
- Security Focus, 195
- Security information, disseminating, 80–81
- Security lists, joining, 81
- Security patches, applying, 31
- Security tools, developing into products, 81
- SecurityFocus (Symantec), 224
- Security-related organizations, 191–94
- Senior management, notifying of an attack, 13, 16
- Sequel Technology Corporation, 224
- ServGate, 223
- Shake Communications, 195
- Shavers, Michelle, 137–38
- Schultz, Gene, 1
- Silanis Technology, 224
- SilentRunner Inc., 224
- Silicon Defense, 224
- Sink-or-swim approach to security, 133
- Site Security Handbook, 194

- Smith, Fred Chris, 111
 - Snooping tools, 139
 - SNORT, 200
 - Socks, 200
 - Software, 198–202
 - Solaris Security Toolkit, 200
 - SonicWALL, 224
 - SourceFire, 224
 - Spam, 141
 - Spectrum Systems, 107
 - SPI Dynamics, 225
 - Spitzner, Lance, 53
 - SSH Communications Security, 225
 - Standard architecture designs, using, 63
 - Stonebridge, 225
 - Stonesoft, 225
 - Stratum8 Networks, 225
 - Strossen, Nadine, 135
 - Sun Microsystems, 226
 - SurfControl, 225
 - Swatch, 201
 - Sygate Technologies, 226
 - Symantec, 226
 - System administrators, 49
 - executive-level security summaries issued by, 47–48
 - making training a requirement for, 80
 - responsibilities, 64–65
 - and training budget, 114–15
 - System dump, 14
 - System flaws, 31
 - System snapshot, 14
- T**
- Tally Systems, 226
 - Talos Technology Consulting, Inc., 226
 - TCP Wrapper, 201
 - Technical Communications Corporation, 227
 - TenFour U.S. Inc., 227
 - Thawte Certification, 227
 - Thrupoint, 227
 - Tiger, 201
 - TippingPoint Technologies, 227
 - TIS Firewall Toolkit, 201
 - Titan, 201
 - Tivoli Software (IBM), 227
 - T-NETIX, 226
 - Top Layer, 228
 - Training, 71–82
 - budget, protecting, 79
 - checklist, 81–82
 - executive management, educating, 79
 - in incident-response procedures, 13
 - Intermint Financial case study, 72–78
 - lunch-hour seminars, 80
 - for management, making a requirement, 79
 - overlooking, 72–78
 - providing, 49
 - security, 32
 - security information, disseminating, 80–81
 - security lists, joining, 81
 - security tools, developing into products, 81
 - for system administrators, making a requirement, 80
 - white papers, writing, 81
 - TransWorld Internet Services case study, 21–27
 - discovery of a hacker, 23
 - false sense of security, 22–23
 - fixing security, 23–25
 - network at risk, 25–26
 - Trend Micro, Inc., 228

- Trintech Group, 228
 - Tripwire, Inc., 201, 228
 - Trojan horses, 141
 - TruSecure, 228
 - TrustWorks, 228
 - TTY-Watcher, 201
 - Tumbleweed Communications Corporation, 228
- U**
- Ubizen, 229
 - Unisys, 229
 - Unknown attacks, 11
 - Unnecessary services, disabling, 65
 - Unplanned security, 85–96
 - budget cuts, 93–94
 - checklist, 95
 - keeping score, 95
 - learning from the past, 93
 - management, holding accountable, 94
 - risk assessment, 92
 - Rockland General case study, 86–92
 - security testing, 94
 - system classification, 93
 - training, 94–95
 - trust, 93
 - Unsecured email, 137–42
 - email hazards, 141–42
 - encryption, 138–41
 - personal data, access of, 138–39
 - waiving your right to privacy, 139–40
 - Unsecured systems:
 - connecting to the Internet, 66
 - and executive support, 39–40
 - U.S. Office of Homeland Security, 194
 - U.S. Secret Service, 197
 - USENIX, 80, 194
- V**
- Vanguard Integrity Professionals, 229
 - Vasco, 229
 - VeriSign, 229
 - Viruses, 141
 - Vogon, 63
 - V-ONE Corporation, 229
- W**
- WatchGuard Technologies, Inc., 230
 - White papers, writing, 81
 - WinMagic Inc., 230
 - Worms, 141
 - Written policy, for dealing with break-ins, 13–14
- Y**
- Yahoo!, 29
- Z**
- Zero Knowledge Systems, 230
 - Zero-day attacks, 11
 - Zone Labs, Inc., 230