



Index

A

Access. *See also* Unauthorized access
 described, 44, 285
 increased, 48

Account(s)
 default, 60–64
 described, 45

Actions, described, 44

Address Resolution Protocol. *See* ARP
 (Address Resolution Protocol)

Advertising, of non-business related activities,
 37–38

Advisories. *See also* Notification
 CERT CC, 26, 177, 178
 writing, 178–180

Agents, autonomous, 47

Aimpw, 62

Amazon.com, 23

American Cancer Society, 75

American Megatrends, 62

American Registry for Internet Numbers. *See*
 ARIN (American Registry for Internet
 Numbers)

Andress, Mandy, 103

Antivirus software, 33, 70. *See also* Viruses

AOL Instant Messenger, 62

APNIC (Asian Pacific Network Information
 Center), 282

Application-perspective scanning tools, 140

Architectural reviews, 25, 285

ARIN (American Registry for Internet Num-
 bers), 282

ARP (Address Resolution Protocol), 93

Asian Pacific Network Information Center. *See*
 APNIC (Asian Pacific Network Infor-
 mation Center)

Assessment, described, 134

ATF (Bureau of Alcohol, Tobacco, and Fire-
 arms), 209, 212

Attack(s). *See also* Attackers; DoS (Denial-of-
 Service) attacks; Incidents
 brute-force, 61, 62
 buffer-overflow, 67, 68
 consequences of, 57–59
 described, 46, 55–78
 full-knowledge, 134–135
 human factors related to, 60–65, 142
 physical, 46
 social-engineering, 64, 129–130, 289
 vectors, 60–68
 wireless, 64–65

Attackers. *See also* Attacks; Hackers
 described, 48
 motivation of, 49
 types of, 48–49

Auditing, 32, 134, 285

AusCERT (Australia Computer Emergency
 Response Team), 5, 8, 141

Authentication, 44, 285

Autonomous agents, 47

B

Back Orifice, 73

Backups, 146, 151, 156, 165–166, 196,
 229–230

Baker, Richard, 26

Betts, Bill, 224

Bindview, 139

!Bios, 62

“Black box” testing, 137

BO2K (Back Orifice 2000), 73

Boot-sector viruses, 71

brute-force attacks, 61, 62

- BTCERTCC (British Telecommunications CERT Coordination Center), 8
- Buffer-overflow attacks, 67, 68
- Bugtraq, 135
- Bureau of Alcohol, Tobacco, and Firearms (ATF), 209, 212
- Business
- cases, establishing, 109
 - partners, 124
 - units, 123
- Buy.com, 23
- Bypass, described, 45
- C**
- Cain, 62
- Canada, 8
- Carnegie Mellon University, 4
- CARNet CERT (Croatian Academic and Research Network CERT), 8
- CBK (Common Body of Knowledge), 113
- CERT (Computer Emergency Response Team). *See also* CERT CC (CERT Coordination Center)
- described, 3–4, 286
 - formation of, 2–3
 - IRTs and, 7, 8
 - Web site, 4
- CERT CC (CERT Coordination Center), 5, 42, 56. *See also* CERT (Computer Emergency Response Team)
- advisories, 26, 177, 178
 - checklists, 141
 - formation of, 4
 - incident tracking and, 175–176
 - report forms, 155, 171–172
 - team credibility and, 27
 - vulnerabilities reported to, 75–76
 - Web site, 44
- CERTCC-KR, 8
- Certifications, 112–116
- CERT-IT, 8
- CERT-NASK (CERT-Research and Academic Network in Poland), 8
- CGI (Common Gateway Interface), 67–68
- Chain mail, 37–38
- Chargeback models, 110
- Checklists, 140–141
- CIAC (Computer Advisory Capability), 5
- CIC (Committee on Institutional Cooperation), 193
- CISA (Certified Information Systems Auditor), 114–115
- Cisco, 140, 188
- CISSP (Certified Information Systems Security Professional) certification, 112–114
- CNN.com, 23
- Code of Ethics, 113
- Coding oversights, 66–68, 132
- Cohen, Fred, 68
- Common Body of Knowledge. *See* CBK (Common Body of Knowledge)
- Common Gateway Interface. *See* CGI (Common Gateway Interface)
- Common sense, importance of, 88–89
- Common Vulnerability and Exposure (CVE) project, 50–51, 53
- Communication(s)
- departments, 123
 - experts, 86
 - plans, 117
 - skills, 91
- Companion viruses, 71
- Components, described, 45
- Compromises, system, 57–59
- Computer, use of the term, 45–46
- Computer Crime and Security Survey, 9–10
- Computer Fraud and Abuse Act, 205
- Computer incidents. *See* Incidents
- Constituencies
- defining, 13–14
 - size of, 80–81
 - training, 116
- Contacts, establishing, 151, 203–204
- Containment, 162–165
- Copying, described, 45
- Copyrights, 39–40, 206
- Cornell University, 3, 205
- Corporate raiders, 49
- Cost, of incidents, 183–199
- Coverage, determining the best, 84–85
- CPU (central processing unit) cycles, 100
- Credibility, importance of, 27
- Criminalistics, 218

- Criminology, 218
 CSI (Computer Security Institute), 8–10, 184–185
Cuckoo's Egg, The (Stoll), 3
 Customer service, 22
 Customs Service (United States), 209, 211
 CVE (Common Vulnerability and Exposure) project, 50–51, 53
 Cyber-terrorism, 123. *See also* Terrorism
- D**
- DARPA (Defense Advanced Research Projects Agency), 3–4
 Data. *See also* Information
 described, 45
 handling, controls over, 131
 tap, 47
 Database administrator role, 85, 94
 Datak Online Web site, 23
Dateline (news program), 74
 Deductive reasoning skills, 91
 Deleting, described, 45
 Department of Homeland Security, 19–20, 123–124
 DFN-CERT, 5
 Diagnostic tools, 99
 Diplomacy, 91
 Disgruntled employees, 37
 DMCA (Digital Millennium Copyright Act), 206
 DNS (Domain Name Service), 93
 DOE-CIAC NIDS, 140
 Domain name
 extensions, 263–282
 Service (DNS), 93
 DoS (Denial-of-Service) attacks
 classification of, as incidents, 29, 32–33, 41
 cost of, 186
 described, 32–33, 48, 59, 286
 notification and, 82–83
 Smurf, 59, 65–66
 statistics on, 9
 testing tools and, 99–100
 tracking, 23–24
 virus hoaxes and, 75
 DOS (Disk Operating System), 226
- E**
- Eavesdropping, 186
 e-Bay, 23
 Einstein, Albert, 217
 E-mail attachments, 75. *See also* Viruses
 Emergency 911 Telephone system, 23
 Employees, disgruntled, 37
 Encase (Guidance Software), 140
 Encryption tools, 106
 Energy Department (United States), 5, 8, 140
 Enterasys Dragon, 140
 Ethics, 113
 E*Trade Web, 23
 Events, described, 44
 Evidence. *See* Forensics
 EWA-Canada/CanCERT, 8
 Excite, 23
- F**
- Facilities, 97–98
 FAQs (Frequently Asked Questions), 236, 257–261
 FAT (File Allocation Table), 226
 Fax machines, 33, 100
 FBI (Federal Bureau of Investigation), 19–20, 56, 209
 described, 286
 jurisdiction of, 210–211
 surveys/statistics, 8–10, 184–185
 types of crimes investigated by, 211
 working with, 18, 123
 Feedback, 172–174
 File infector viruses, 70
 File Transfer Protocol (FTP), 93, 284
 Financial records, 37
 Finger, 99
 Fire departments, 123
 FIRST (Forum of Incident Response and Security Teams), 5–8, 179
 Flooding, 44, 286
 Focus, of CIRT efforts, 13–16
 Forensics
 challenges facing, 221–223
 described, 215–232, 286
 methodologies, 227–230
 tools, 103–105, 140

Freedom of Information Act, 157
 FTC (Federal Trade Commission), 210, 212
 FTP (File Transfer Protocol), 93, 284
 Full-knowledge attacks, 134–135

G

Gammalog, 62
 GIAC (Global Information Assurance Certification), 91, 115–116, 286
 Giuliani, Rudolph, 150–151
 Goodwill, loss of, 192
 Guidance Software, 140

H

Hackers, 48, 194. *See also* Attackers
 Heiser, Jay G., 224
 Help desk personnel, 87
 HIDS (host-based intrusion detection systems), 102, 104
 HIPAA (Healthcare Information Portability and Accountability Act), 157, 208
 Host(s)
 -based intrusion detection systems (HIDS), 102, 104
 scanning, 36, 139
 Howard, John, 42–43, 49–50, 52
 HTML (HyperText Markup Language), 67–68
 HTTP (HyperText Transfer Protocol), 68, 93, 284
 Human factors, related to attacks, 60–65, 142

I

IANA (Internet Assigned Numbers Authority), 282, 283
 IBM (International Business Machines), 5, 62
 ICAMP (Incident Cost Analysis and Modeling Project), 193–199
 ICANN (Internet Corporation for Assigned Names and Numbers), 282
 ICMP (Internet Control Message Protocol), 33, 66, 93
 ICSA Labs, 34

Identification

badges, 58
 phase, 145

IDS (intrusion detection system), 20, 22–23, 101–103, 136, 139–140, 170. *See also* Intrusion

I Love You virus, 34

Incident(s). *See also* Attacks

analysis, 93, 145, 159–161, 168–169
 categories for, determining, 40–41
 cost of, 183–199
 counting, 23–24
 described, 29–41, 48, 50–51
 handling, 85, 88–94, 148–149
 identifying/defining, 21, 153–156
 operational versus security, 39–40
 response life cycles, 144–171
 sample, 168–171
 taxonomy, 42–50
 tracking, 21–23, 174–176
 triage, 22

Information. *See also* Data

corruption of, 48
 disclosure of, 48
 exchange, 46

Information Security (magazine), 133, 224

InfraGard, 19–20, 178, 287

Integrity, 91, 287

Intellectual property, 39–40, 206

Internetworks, 46

InterNIC (Internet Network Information Center), 91, 282

Interviews, personnel, 96–97, 107, 125–126

Intrusion(s), @ IDS (intrusion detection system)

attempted, 32
 classification of, as incidents, 31–32
 consequences of, 57–59
 successful, 31–32, 41

IP (Internet Protocol)

addresses, 23, 60, 163, 241, 263
 familiarity with, importance of, 91
 hopping, 82–83

IRSTs (incident response and security teams), 6

IRTs (incidence response teams), 7–8

- ISACA (Information Systems Audit and Control Association), 114, 115, 287
- ISC (International Information Systems Security Certification Consortium), 112, 113, 114
- ISPs (Internet Service Providers), 23, 156, 170–171
- ISRT (information security response team), 8
- ISS (Internet Security Systems), 5, 139, 140
- Italy, 8
- J**
- Jaz drives, 105
- John the Ripper (program), 62
- Justice Department (United State), 152, 188–189, 204–205, 209–210, 243
- K**
- KGB (Soviet Union), 3
- Korea, 8
- Kruse, Warren G., 224
- L**
- L0phtcrack, 61
- LAN-CERT (Israeli Academic CERT), 8
- Laptop(s)
- theft of, 186
 - unauthorized use of, 38
- Law enforcement, 17–20, 36, 87, 123–124. *See also* Legal community; *specific agencies*
- Lawrence Berkeley Laboratories, 3
- LC4, 61
- Legal community, 85, 95, 192, 201–214. *See also* Law enforcement; Legislation
- Legal departments, 122. *See also* Legal community
- Legislation, 204–208, 243–256. *See also* Law enforcement; Legal community
- Digital Millennium Copyright Act (DMCA), 206
 - Freedom of Information Act, 157
 - Healthcare Information Portability and Accountability Act (HIPPA), 157, 208
 - Patriot Act, 243
- Lessons learned phase, 145, 166–171
- License violations, 39
- Logic bomb programs, 37, 73, 287
- Logs, 150, 197, 273, 287
- Longstaff, Thomas A., 42–43, 49–50, 52
- LoveLetter virus, 34, 73
- M**
- Macro viruses, 71, 75
- Malicious logic, 33, 40, 93, 189. *See also* Viruses
- described, 68–75
 - experts, 86
- Marketing, 107, 116–118, 123
- MD5 checksums, 27, 66–67, 164, 179–180, 226
- Media, dealing with, 118–119, 212–213, 222
- Melissa virus, 34, 187, 189
- Metacharacters, 68
- Meunier, Pascal, 42
- Microsoft
- checklists, 141
 - Configuration and Analysis Snap-In, 139
 - SQL Server, 62
 - Windows, 56, 61, 62
- Mission statements, 13–28
- Mitre Corporation, 51
- Modifying, described, 45
- Morris, Robert T., Jr., 3, 73, 205
- MSSPs (managed security service providers), 83, 287
- Mssqlpwd, 62
- Multipartite viruses, 71
- N**
- NAAG (National Association of Attorneys General), 210
- NASA (National Aeronautics and Space Administration), 3
- NESSUS, 136, 139
- Netbus, 73
- Network(s)
- based intrusion detection systems, 102, 104
 - File System (NFS), 93
 - interfaces, common oversights in, 67–68

- Network(s) (*cont.*)
 monitors, 103
 operating center (NOS), 97–98
 scanning/probing, 36, 41, 44, 59–60, 139, 288
 use of the term, 46
 “Newspaper effect,” 132–133
 NFR Intrusion Management System, 140
 NFS (Network File System), 93
 NIPC (National Information Protection Center), 19–20
 NIST (National Institute of Standards and Technology), 141
 NOC (network operating center), 97–98
 Norton AntiVirus (Symantec), 70
 Notification, 82, 145, 156–159, 168, 169. *See also* Advisories
 NSA (National Security Agency), 141
- O**
- Objectives, described, 48
 Omega Engineering Corporation, 185
 Omni Consulting Group, 199
 Operating systems
 number of, ratio of experts per, 81
 weaknesses of, 132
 Operational strategy, 20–24
 Outsourcing, 83
- P**
- PalmCrack, 62
 Parmalee, George, 233
 Partition-sector infector viruses, 70
 Passwords, 32, 60–64
 changing, 60–61, 163
 cracking, 61, 62, 101
 selecting, 63–64, 130
 Patience, importance of, 88
 Penetration testing, 25, 99–101, 133–138, 148, 151–152, 287
 PGP (Pretty Good Privacy), 62
 PGPPASS, 62
 PHRACK, 135
 Physical security, 46, 123, 131–132, 194
 PkCrack, 62
 PKZIP files, 62
 Policies, 142–143, 146–150, 194, 288
 Polymorphic viruses, 71
 POP (Post Office Protocol), 62
 Pornographic material, 35–36, 41
 Ports, 59–60, 283–284
 Postal Inspection Service (United States), 209, 211
 Postal Service (United States), 8, 187, 209–211
 Practices, sound, 131–132
 Preparation phase, 145, 146–153
 Press, dealing with the, 118–119, 212–213, 222
 Probes, 36, 41, 44, 59–60, 288
 Problem-solving skills, 91
 Procedural controls, 132
 Processing, described, 45
 Professional criminals, described, 49
 Program, use of the term, 46–47
 Programming oversights, 66–68, 132
 Promotions, 95–96
 Protocol(s). *See also specific protocols*
 analyzers, 103
 familiarity with, importance of, 91–92
- R**
- RAID (Redundant Array of Inexpensive Disks), 229
 RAM (Random-Access Memory), 226, 229
 Ramsland, Katherine, 217
 RARP (Reverse Address Resolution Protocol), 93
 Reading, described, 45
 RealSecure (Internet Security Systems), 140
 Recall procedures, 146
 Recovery, 145, 165–166, 169, 170–171. *See also* Backups
 Registry (Windows), 62
 Remediation, 145, 161–165, 169, 170
 Remnant files, 150, 288
 Reports, 155, 167–168, 171–176, 209–213, 239–242

- Research and development, 26–27, 86
- Resources, theft of, 34–35, 41, 48, 191, 186
- Response(s)
 - defining, in mission statements, 15–16
 - guidelines, 150–151
- Reverse Address Resolution Protocol (RARP), 93
- Rezmierski, Virginia, 193
- Risk
 - analysis, 153
 - assessment, 25, 108–109, 288
 - described, 288
 - methodology tools, 141
- Role playing, 96
- ROM (Read-Only Memory), 226

- S**
- Sabotage, 37, 41, 186
- Safeguards, 108
- Safety concerns, 81
- SAINT (Security Administrator's Integrated Network Tool), 136, 139
- Sandia National Laboratories, 42
- SANS (SysAdmin, Audit, Network, Security) Institute, 115, 116
 - checklists, 141
 - conferences, 111, 178
 - described, 56
- SARA (Security Auditor's Research Assistant), 139
- Scanning, 36, 41, 44, 139
- Science, use of the term, 216
- Scope, of CIRT efforts, 13–16
- Scripts, 46–47
- Search warrants, 217–218
- SEC (Securities and Exchange Commission), 210, 212
- Secret Service (United States), 123, 209, 210, 211
- SEI (Software Engineering Institute), 4
- sendmail, 66
- Services
 - coverage options and, 80–83
 - provided, number of, 80
- Shareholders, 192

- Shift leaders, 87
- Signature files, 34, 68–69, 70, 75, 226–227
- Slammer virus, 34
- Slurpie, 62
- SMTP (Simple Mail Transfer Protocol), 46, 284
- Smurf (DoS attack), 59, 65–66
- SNORT, 140
- SOC (security operations center), 87, 90, 97–98
- Social-engineering attacks, 64, 129–130, 289
- Soviet Union, 3
- SPAN network, 6
- Spies, described, 48
- Split coverage, 83
- Spoofing, 45, 289
- SQL injection, 68
- SQL Server (Microsoft), 62
- SSCP (System Security Certified Practitioner) certification, 113–114
- Staffing. *See also* Teams
 - coverage options and, 80–83
 - partial on-site, 81–83
 - 24 × 7, 80–81
- Statistics, 8–10, 153, 184–189, 234
- Stealing, described, 45
- Stoll, Clifford, 3
- Storage media, 225–226
- Subject matter experts, 86
- SWOT analysis, 117
- Symantec, 70, 139
- SYN-ACK signals, 65, 135–136
- System
 - administrators, 86, 132–133
 - restoration, 165–166, 169, 170–171

- T**
- Targets, described, 44
- Taxonomy, of computer incidents, 42–50
- TCP (Transmission Control Protocol), 91, 137
- TCP/IP (Transmission Control Protocol/Internet Protocol), 65–66, 135
- TCT (The Coroner's Toolkit), 140
- Team(s). *See also* Staffing
 - assembling, 80–83

Team(s) (*cont.*)

- building exercises, 126–127
 - cohesiveness of, 126–127
 - effectiveness of, 121–129
 - external members of, 122–125
 - funding, 106–110
 - growth within, providing for, 95–96
 - internal, 83, 125–128
 - interviewing candidates for, 96–97, 107, 125–126
 - leaders, 89–90, 94
 - marketing, 116–118
 - MSSP and, 83
 - placement of, 109–110
 - promotions within, 95–96
 - retaining members of, 126–127
 - roles, 85–88
 - skills, 88–95
- TELNET, 46, 93, 284
- Terminology, 29–54, 235
- Terrorists, 49, 123
- Testing
- penetration, 25, 99–101, 133–138, 148, 151–152, 287
 - types of, 133–134
- TFTP (Trivial File Transfer Protocol), 32
- Threads, 108
- “Time bomb” programs, 187
- Tool(s)
- described, 46–47, 99–106
 - diagnostic, 99
 - encryption, 106
 - forensics, 103–105, 140
 - intrusion detection, 101–103, 104
 - kits, 47, 140
 - selecting, 129–142
- Training, 110–116, 129–131, 153, 194
- Transmission Control Protocol (TCP), 91, 137
- Transmission Control Protocol/Internet Protocol (TCP/IP), 65–66, 135
- Trojan horses
- classification of, as incidents, 33–34, 40, 41
 - coding oversights and, 66–67
 - described, 33–34, 73, 289
- Trouble ticket system, 174
- Trust relationships, 163

U

- UDP (User Datagram Protocol), 93
- Unauthorized access, 37–38, 93. *See also*
- Access
 - classification of, as an incident, 31–32, 41
 - consequences of, 57–59
 - described, 31–32
 - examples of, 168–169
 - unsuccessful, 32, 41
- Unauthorized results, 46–48
- University of Michigan, 193
- UNIX, 46, 56, 62, 66
- Urban legends, 74–75, 289
- URLs (Uniform Resource Locators), 68
- User Awareness training, 25–26
- User commands, described, 46
- User enrollment, 24

V

- Value, use of the term, 108
- Vandals, described, 49
- Vendors, working with, 122–123
- Virus(es)
- biologic viruses and, comparison of, 68–69
 - classification of, as incidents, 29, 33–34, 40, 41
 - cost of, 34, 186, 187, 189
 - described, 33–34, 68–71, 289
 - hoaxes, 74–75, 289
 - preventing, 72
 - statistics on, 10
 - tracking, 34
- VMyths.com, 74
- Voyeurs, described, 49
- VPNs (virtual private networks), 106, 159
- Vulnerabilities
- assessment of, 24, 290
 - CVE project and, 50–51, 53
 - described, 47, 51, 108, 289
 - design, 47
 - implementation, 47
 - list of, 131–132

reported to CERT CC, 75–76
scanning, 99–101
software, 39
testing, 27

W

War dialing, 65, 100
War driving, 65
Warning banners, 152–153
Wazzu virus, 68–70
Webercracker, 62
West German Computer Club (Chaos Club), 3
WHOIS, 99
Windows (Microsoft), 56, 61, 62. *See also* Operating systems
Wireless attacks, 64–65
Wiretapping, 102, 186
Word (Microsoft), 69, 75

World Wide Web
interfaces, common oversights in, 67–68
surfing, unauthorized, 38

Worms, 3, 205
classification of, as incidents, 33–34, 41
described, 33–34, 73, 290
Worst-case scenarios, 110

Y

Yahoo! Web site, 23

Z

ZDNet.com Web site, 23
Zero-knowledge attacks, 134
Zip drives, 105
ZIP files, 62
Zipcrack, 62