

---

# INDEX

---

## A

- Abuse of network resources, 165–166
- Acceptable downtime, 159
- Acceptable-use policies, 181
- Access channels, 306
- Access control
  - to modems, 216–218
  - policies for, 182–183
- Access control lists (ACLs)
  - for HIPAA, 195
  - for worms, 92–93
- Access control servers (ACSs), 53–54,  
61–65, 67
- Access Control standard in HIPAA, 190
- Access logs. *See* Logs
- Access points in wireless networks, 58–59,  
64, 68
- ACK messages, 42
- ACLs (access control lists)
  - for HIPAA, 195
  - for worms, 92–93
- ACSs (access control servers), 53–54,  
61–65, 67
- Address Resolution Protocol (ARP)
  - tables, 6
- Addressable elements in HIPAA, 188
- Administrative safeguards in HIPAA, 189
- ADSL for dosbots, 45
- Advisories for virus attacks, 71
- Agency tasks in disaster incident, 159–162
- Agents
  - in DoS attacks, 45
  - in ESM, 198
- Aggressive timing policy, 20
- AirSnort tool
  - for encryption keys, 60–62
  - interesting packets with, 63
  - for wireless networks, 57, 62
- Alerts
  - for HIPAA, 195
  - for perimeter defense, 135–136
- Allow All rule, 74

INDEX

---

- Allow Any rule, 75
- American National Standards Institute for security policies, 171
- American Registry for Internet Numbers (arin.net), 193
- Analysis
  - in disaster incident, 154–158
  - of evidence, 252–254, 300–304
  - in executive fraud incident, 268
  - of HIPAA, 191, 202–203
  - in perimeter defense, 127–128
- Anomaly-based intrusion detection systems, 34
- Anonymous attachments, 198
- Anonymous FTP sessions, 75–76
- Antennas, 64
- Antistatic wrist straps
  - in cyber extortion incident, 287
  - in industrial espionage incident, 242
- Antivirus software, 75, 79
  - for financial transactions, 144
  - for home systems, 318
  - for worms, 87, 92, 95
- apache daemon, 107
- Apache servers, 108
- Apex Dental company. *See* Security policies
- Application banners
  - identifying, 107
  - in site defacement incident, 114
  - telnet, 12
  - in war dialing, 212
- Application service provider (ASP)
  - business model, 23
- Applications in site defacement
  - assessment, 106
  - identifying, 106
  - log services for, 115
- Arachnids, 137
- Archiving
  - e-mail, 258
  - evidence, 254–255, 304
- Areas menu in TextSearch Plus, 302
- arin.net (American Registry for Internet Numbers), 193
- ARP (Address Resolution Protocol)
  - tables, 6
- Ashley Landscapers. *See* Cyber extortion incident
- ASP (application service provider)
  - business model, 23
- Aspen company. *See* Home architecture incident
- Assessment
  - in disaster incident, 150–151
  - of security policies, 174
  - in site defacement incident, 106–113
  - of virus attack losses, 77–79
- Assigned Security Responsibility
  - standard, 189
- astalavista.box.sk site, 108
- Attachments
  - in HIPAA tests, 198
  - Trojan horses in, 283
- ATTR command, 294
- Audit Controls standard, 190
- Auditing
  - in executive fraud incident, 269, 271
  - operating system differences in, 199
- Authentic evidence, 262
- Authentication
  - of evidence, 248–251, 294–300

- for intellectual assets, 257
  - in war dialing, 217–218
  - in wireless networks, 65, 67
- Authorization for worm attacks, 103
- Automated password processes, 232–233
- Availability for financial transactions, 144
- Awareness
- of HIPAA, 202–203
  - of security policies, 184–186
- ## B
- Back Orifice Trojan horse, 282–283
- Backbones, 84–85
- Backup batteries
- in cyber extortion incident, 287
  - in industrial espionage incident, 242
- Backups
- in disaster incident, 152
  - in evidence acquisition, 243, 247, 289, 293
  - hot sites for, 148
  - off-site storage, 157–158
  - reliability of, 178
  - for virus attacks, 77
  - for worm attacks, 99
- Bandwidth in DoS attacks, 42
- Banking incidents. *See* Perimeter defense; Wireless networks
- Banner grabbers, 194
- Banners
- identifying, 107
  - in site defacement incident, 114
  - telnet, 12
  - in war dialing, 212
- Baselines for virus attacks, 77, 80
- Batteries
- in cyber extortion incident, 287
  - for evidence protection, 272
  - in industrial espionage incident, 242
- BBSs (bulletin board systems), 213
- Behavior in social engineering, 228–230
- “Best evidence” rule, 263
- Bindin tool, 198
- Biomedical research firm virus incident, 69–72
- damage assessment, 77–79
  - lessons learned, 79–81
  - sources of, 72–77
- Biometrics
- in authentication, 218
  - benefits of, 315–316
  - resources for, 325
- Bit stream backups, 243, 247
- BlackBerry devices, 55
- Blank passwords, 198
- Blind scans, 20
- Block zone transfers, 11
- Blocking caller IDs, 215
- Books, 321
- Boot disks in evidence acquisition, 244
- Booting
- in evidence acquisition, 245
  - in virus attacks, 70, 76
- Border protection. *See* Perimeter defense
- Branch offices, security with, 144–146
- Broadcasting SSIDs, 59
- Brute-force connection makers, 110
- Brute-force log ins, 211
- Brutus tool, 110

INDEX

---

- Budgets
    - for perimeter defense research, 131
    - for wireless networks, 54
  - Buffer overflows, 108, 111
  - BugTraq tool, 137
  - Bulletin board systems (BBSs), 213
  - Business Associate Contracts standard, 189
  - BWell Clinics case. *See* Health Insurance Portability and Accountability Act (HIPAA)
- C**
- Cable modems for dosbots, 45
  - CAC (Common Access Card), 313
  - Call timeout settings in war dialing, 210
  - Caller IDs, blocking, 215
  - Camel tool, 15–16
  - Cameras for evidence
    - in cyber extortion incident, 287, 306
    - in executive fraud incident, 272
    - in industrial espionage incident, 242
  - Capturing hard drives, 306
  - CAs (certificate authorities), 310
  - Cassette recorders
    - in cyber extortion incident, 287
    - in industrial espionage incident, 242
  - CD-ROMs for virus attacks, 80
  - Center for Internet Security (CIS), 195
  - Central information centers in disaster incident, 151
  - Central repositories for network configurations, 156
  - Certificate authorities (CAs), 310
  - Chain of custody (COC) forms
    - in cyber extortion incident, 284–289
    - in executive fraud incident, 271–274
    - in industrial espionage incident, 240, 242–243, 251, 259–262
  - Cold storage, 157–158
  - Common Access Card (CAC), 313
  - Common Vulnerabilities and Exposures (CVE), site for, 137
  - in executive fraud incident, 271–274
  - in industrial espionage incident, 240, 242–243, 251, 259–262
- Changes, documenting, 243
  - Changing usage patterns, 34
  - Checksums
    - in executive fraud incident, 275
    - in industrial espionage incident, 248–251, 294–300
  - Chicken wire in wireless networks, 64
  - China worm, 71
  - Chknull tool, 198
  - CIS (Center for Internet Security), 195
  - Claims processing company. *See* Security policies
  - Classes, IP address, 9–10
  - Cleaning
    - hard drives, 268–269
    - hosts, 138
  - Clients
    - in DoS attacks, 45
    - for HIPAA, 192–193
    - in home architecture incident, 28
  - CMOS information
    - in cyber extortion incident, 290–292
    - in industrial espionage incident, 245–246
  - COC (chain of custody) forms
    - in cyber extortion incident, 284–289
    - in executive fraud incident, 271–274
    - in industrial espionage incident, 240, 242–243, 251, 259–262
  - Cold storage, 157–158
  - Common Access Card (CAC), 313
  - Common Vulnerabilities and Exposures (CVE), site for, 137

- Communication of trade secrets clause, 257
  - Company confidential information, 182
  - Company private information, 182
  - Compliance monitoring for HIPAA, 199, 202
  - Components in PKI, 308–309
  - Computer forensics
    - cases. *See* Cyber extortion incident;
    - Executive fraud incident;
    - Industrial espionage incident
    - resources for, 324
  - Computers in site defacement assessment, 106
  - Con games. *See* Social engineering
  - Confidential information, 182. *See also*
    - Industrial espionage incident
  - Confidential intellectual assets, 257
  - Confidentiality for financial transactions, 144
  - Configuration
    - central repositories for, 156
    - documenting, 242–243, 288
  - Consoles in ESM, 198
  - Contact information in social engineering, 226
  - Contact system owners for perimeter defense, 137
  - Contingency plans
    - in HIPAA, 189
    - for worm attacks, 100
  - Continuity of operations plans, 100
  - Continuous-search option, 303
  - Control numbers for evidence, 259–260
  - Corporate fraud. *See* Executive fraud incident
  - Costs
    - of wireless networks, 54
    - of worm attacks, 96
  - Covered entities in HIPAA, 187
  - CPU utilization in virus attacks, 69–70, 76
  - Crackers, 214
  - Cracking tools, 57
  - CRC checksums, 248–251, 294–300
  - CRCMd5 tool, 248, 251, 294
  - Crime teams, 28
  - Crisis management, 161
  - Cross-certification in PKI, 310
  - CSI/FBI Computer Crime and Security Survey, 140
  - Customer satisfaction, downtime effects on, 159
  - Customer support
    - in perimeter defense research, 131
    - social engineering of, 227–230, 233
  - CVE (Common Vulnerabilities and Exposures), site for, 137
  - Cyber extortion incident, 281
    - chain of custody, 284–288
    - evidence
      - acquiring, 288–293
      - analyzing, 300–304
      - archiving, 304
      - authenticating, 294–300
      - incident background, 281–284
      - lessons learned, 305
      - new forensics tools, 305–306
  - Cyber forensic group, 124
  - Cyber security incidents, 207
- D**
- D flag, 20
  - Daemons
    - identifying, 106–107
    - versions, 108
  - Data centers in worm incident, 84–85

INDEX

---

- Data classification policies, 182
- Data integrity
  - in financial transactions, 144
  - in home architecture incident, 28
- data\_length option, 14
- Data losses from worm attacks, 97
- Data mirroring, 162
- Data rate limits, 43
- Data redundancy, 146
- Database Scanner tool, 95, 200
- Databases for HIPAA, 199–200
- Date and time documentation, 245–246, 291–292
- .DBF files, 253
- DD function, 268–269, 273, 275
- DDoS (distributed denial-of-service) attacks, 40–41, 45–47
- Decoy scans, 19–20
- Default passwords in war dialing, 209, 212
- Deleted files in executive fraud incident, 277
- Demilitarized zones (DMZs)
  - for HIPAA, 194–195
  - in home architecture, 25
  - logical connections from, 5–6
  - in target networks, 4–5
  - in virus attacks, 78
  - for war dialing, 219
  - in wireless networks, 68
- Denial of service (DoS) attacks, 37
  - detecting, 124
  - discovering, 37–43
  - lessons learned, 47–49
  - process, 44–47
  - references for, 50
  - resources for, 322
  - response to, 43–44
  - in site defacement assessment, 108
- Dental care insurance provider case. *See* Security policies
- Deny All rule, 72–74, 80
- Department of Defense security standards, 55, 120
- Department of Justice evidence standards, 262–263
- Department on Aging worm incident. *See* Worm attacks
- Destination IP addresses, 138
- Detection requirements in perimeter defense, 126–127
- Device and Media Controls standard, 190
- DHCP (Dynamic Host Configuration Protocol)
  - for IP address allocation, 10–11
  - in perimeter defense, 122
- Dial-back, 217
- Dialing attacks. *See* War-dialing attacks
- Digest information in evidence
  - authentication, 248–251, 294–300
- Digital lines for war dialing, 219–220
- Digital pictures for evidence
  - in cyber extortion incident, 287, 306
  - in executive fraud incident, 272
  - in industrial espionage incident, 242, 259
- Digital-to-analog converters, 220
- Directional antennas, 64
- Disaster incident, 143
  - analysis, 154–158
  - company background, 143–149
  - incident description, 149–154
  - lessons learned, 162–163
  - solution, 158–162

- Disaster recovery
    - plans for, 147–150, 154–156, 158, 161
    - resources for, 323
  - Disaster recovery teams, 148
  - Disclaimers, e-mail, 257
  - Disk drives. *See* Hard drives
  - Disk-to-disk acquisition, 245
  - DISKCOPY command, 247, 293
  - DiskMgr tool, 247, 292
  - DiskSearch Pro tool, 306
  - Disposal, e-mail, 258
  - Distributed denial-of-service (DDoS)
    - attacks, 40–41, 45–47
  - Distributed-system architecture, 146
  - DMZs. *See* Demilitarized zones (DMZs)
  - DNSs (domain name servers)
    - with branch offices, 146
    - in DMZs, 4
    - port scans with, 10
    - zone transfers with, 10–11
  - Documentation
    - centralized servers for, 156
    - chain of custody forms, 259–262
    - configuration, 242–243, 288
    - in disaster incident, 150–151
    - in evidence acquisition, 245–246, 291–292
  - Domain authentication, 65, 67
  - Domain controllers in HIPAA tests, 197
  - Domain name servers (DNSs)
    - with branch offices, 146
    - in DMZs, 4
    - port scans with, 10
    - zone transfers with, 10–11
  - DoS attacks. *See* Denial of service (DoS) attacks
  - DOS redirection, 246, 292
  - Dosbots, 45–47
  - Downtime, 159
  - Drive/Path option in TextSearch Plus, 302
  - Drives. *See* Hard drives
  - DSL for dosbots, 45
  - Dual-homed hosts, 23, 30–31, 35
  - DumpSec tool, 197
  - Dynamic Host Configuration Protocol (DHCP)
    - for IP address allocation, 10–11
    - in perimeter defense, 122
- E**
- E-commerce company incident. *See* Disaster incident
  - E-mail and attachments
    - in DoS attacks, 38
    - in evidence analysis, 254
    - in HIPAA tests, 198, 201
    - in home architecture incident, 27–28
    - policies for, 257–258
    - Trojan horses in, 283
    - in worm attacks, 94, 102
  - EAP (Extensible Authentication Protocol), 61, 63
  - Egress filtering
    - for DoS attacks, 47–48
    - Web site for, 50
  - EnCase Forensic Edition software, 275–277, 306
  - Encryption in wireless networks, 55, 60, 62–63, 65–67
  - End user questions in security policy development, 177

INDEX

---

- Enforcement of security policies, 186
  - Enterprise Security Manager (ESM), 198–199
  - ERP applications, 30
  - Espionage. *See* Industrial espionage incident
  - Ethereal tool
    - for DoS attacks, 39
    - recording load information, 39
    - Web site for, 50
    - for wireless networks, 60–61
  - Evaluation in perimeter defense research, 130, 133
  - Evaluation standard in HIPAA, 189
  - Evidence, 240–242
    - acquiring, 242–247, 271–274, 288–293
    - analyzing, 252–254, 300–304
    - archiving, 254–255, 304
    - authenticating, 248–251, 294–300
    - chain of custody forms for, 259–262
    - Federal guidelines for, 262–263
  - Evidence labels, 242
  - Executive fraud incident, 265–266
    - allegation, 269–270
    - drive imaging in, 273–275
    - evidence collection, 271–274
    - investigation preparation, 266–267
    - lessons learned, 279–280
    - logical file structures, 275–277
    - reporting in, 278–279
    - smoking gun in, 278
    - unallocated space and file slack in, 277–278
    - whistle-blower in, 266–267
  - Exit strategies for social engineering, 231
  - Extended Phone Operations Tool (XPOT), 209–210
  - Extensible Authentication Protocol (EAP), 61, 63
  - External perimeters for HIPAA, 191
  - External reviews for HIPAA, 193–196
  - Extortion. *See* Cyber extortion incident
- ## F
- F flag, 14
  - Facilitated risk analysis, 158
  - Facility Access Controls standard, 190
  - Family Educational Right and Privacy Act (FERPA), 188
  - FAQs for security policies, 185
  - FastBloc acquisition, 245
  - FAT32 file system, 247, 292
  - Federal evidence guidelines, 262–263
  - Feedback loops for worm attacks, 100
  - FERPA (Family Educational Right and Privacy Act), 188
  - File attributes, 294
  - file names for investigations, 304
  - File slack
    - in cyber extortion incident, 301
    - in executive fraud incident, 277
    - in industrial espionage incident, 252
  - File structures, 275–277
  - FileList utility, 253
  - Filter\_I tool, 252
  - Filters
    - for DoS attacks, 47–48
    - Web site for, 50
    - in wireless networks, 65–66
  - FIN scans, 18–19



- Financial institution incidents. *See*  
Disaster incident; Perimeter defense;  
Wireless networks
- Financial loss in disaster incident, 160
- Fingerprinting target networks, 4
- Fingerprints in authentication, 218, 315
- Fire incident. *See* Disaster incident
- Firefighting units for worm attacks, 99
- Firewalls  
description, 316  
detecting, 18–19  
in DoS attacks, 38  
hiding from VisualRoute, 18  
for HIPAA, 194  
for home systems, 318  
in perimeter defense, 122  
port 80 on, 8  
resources for, 325  
in target networks, 4–6  
for virus attacks, 72–74, 80  
for worm attacks, 87, 92–93, 99
- Flexibility in disaster recovery, 162
- Flooding in DoS attacks, 41
- Flowcharts for worm attacks, 100–101
- Forensics  
cases. *See* Cyber extortion incident;  
Executive fraud incident;  
Industrial espionage incident  
resources for, 324
- Forwarding electronic mail, 258
- Fraud. *See* Executive fraud incident
- Free space  
in cyber extortion incident, 301  
in executive fraud incident, 277  
in industrial espionage incident, 252
- FTP sessions, virus attacks from, 75–76
- G**
- g flag, 13
- GetFree tool, 252, 301
- GetSlack tool, 252, 301
- GETTIME.DOC file, 246, 291–292
- GetTime utility, 245–246, 291–292
- GLBA (Gramm-Leach-Bliley Act), 188
- Golden CDs, 80
- Government agencies  
IDSs for, 119  
worm incident. *See* Worm attacks
- Grabbb tool, 12–13
- Gramm-Leach-Bliley Act (GLBA), 188
- Groups for security policy development,  
168–169
- Guessing passwords, 109, 211
- H**
- Hackers in home architecture incident,  
32–33
- Hacking scripts, 221
- Hailstorm product, 133
- Handheld devices  
in HIPAA tests, 201  
in worm attacks, 103
- Handlers in DoS attacks, 45
- Handshakes in DoS attacks, 42
- Hard drives  
capturing, 306  
in evidence acquisition, 243, 246, 290, 292  
in evidence authentication, 251, 300  
in executive fraud incident, 267–269,  
273–275  
swapping, 300  
in virus attacks, 69

INDEX

---

- Health and safety, downtime effects on, 159
  - Health Insurance Portability and Accountability Act (HIPAA), 180, 182, 187–191
  - analysis, 202–203
  - assessment, 191
    - client, 192–193
    - external reviews, 193–196
    - internal reviews, 196–201
  - conclusion, 204
  - consequences, 203
  - resources for, 323–324
  - solutions, 203
- Help desk
- call reductions to, 314
  - social engineering of, 227–230
- Hermes chipsets, 57
- Hiding scans, 19–21
- Hiring process, intellectual asset protection in, 256
- Home architecture incident, 23–24
- background, 24–25
  - disclosure, 28
  - e-mail in, 27–28
  - investigation, 28–29
  - lessons learned, 33–36
  - monthly bill in, 26–27
  - reconstructing, 29–31
  - repercussions, 32–33
  - response, 33
- Home security, resources for, 326
- Home users, 317–318
- host\_timeout flag, 20
- Hosts
- dual-homed, 23, 30–31, 35
  - in home architecture incident, 35
  - for perimeter defense, 138
  - zombie, 20–21
- Hot fixes for DoS attacks, 47
- Hot network jacks, 103
- Hot sites, 148, 152–153
- HPFS file system, 247, 293
- HTML-based e-mails for worm attacks, 102
- HTTP (Hypertext Transfer Protocol) port scans, 10
- httpd daemon, 106–109
- Hubs with worms, 95
- Human resources actions in disaster incident, 161
- Hypertext Transfer Protocol (HTTP) port scans, 10

**I**

- i flag, 13
- IANA (Internet Assigned Numbers Authority), 137, 306
- Icebreakers, 169
- ICMP (Internet Control Message Protocol), 15
- ICMP-time-exceeded message, 18
- ICMP traffic, monitoring, 39
- Identifying questions in social engineering, 233
- Identity management (IM)
  - description, 311–312
  - resources for, 325
- Identity theft
  - description, 318–319
  - resources for, 326
- Idlescans, 20
- IDSs. *See* Intrusion detection systems (IDSs)

- iL flag, 14
- IM (identity management)
  - description, 311–312
  - resources for, 325
- Image loss from worm attacks, 98
- Images, disk drive, 243, 247, 273–275, 290, 293
- IMAP port scans, 11
- Implementation requirements in perimeter defense, 129
- Important data classification, 182
- In-house vs. outsourcing in PKI, 310
- Incident response units, 115
- Incident tracking system (ITS), 262
- Indexing tools for evidence analysis, 253
- Industrial espionage incident, 237
  - company background, 237–242
  - evidence
    - acquiring, 242–247
    - analyzing, 252–254
    - archiving, 254–255
    - authenticating, 248–251
    - intellectual asset protection, 255–259
    - lessons learned, 255
- Information Access Management
  - standard, 189
- Information disclosure procedures, 258–259
- Ingress filtering
  - for DoS attacks, 47–48
  - Web site for, 50
- Initialization vectors, 60
- Insane timing policy, 20
- Insider abuse, 165–166
- Installation base in perimeter defense
  - research, 131
- Insurance companies. *See* Disaster incident; Security policies
- Integration requirements in perimeter defense, 129
- Integrity
  - in financial transactions, 144
  - in home architecture incident, 28
- Integrity standard in HIPAA, 190
- Intellectual assets. *See* [u] *Industrial espionage incident*
- IntelliSearch option, 303
- Internal intellectual assets, 256
- Internal reviews for HIPAA, 196–201
- Internal systems for HIPAA, 191
- Internet Assigned Numbers Authority (IANA), 137, 306
- Internet Control Message Protocol (ICMP), 15
- Internet Relay Chat (IRC) programs, 45–47
- Internet Software Marketing Ltd., 171
- Internet Storm Center, 137
- Interviews
  - for perimeter defense, 124, 131
  - for security policies, 173, 177–180
- Intrusion detection systems (IDSs)
  - DMZ monitoring by, 5
  - for DoS attacks, 48
  - in home architecture incident, 34
  - importance of, 21
  - for perimeter defense. *See* Perimeter defense
  - resources for, 323
  - for virus attacks, 75
  - Web site for, 50
  - for worms, 87, 92, 99
- “Intrusion Detection Systems” standard, 123

**INDEX**

---

- Intrusion monitoring, 66
  - Investigative team for executive fraud, 266–267, 269
  - IP addresses
    - DHCP for, 11
    - in DoS attacks, 42
    - fake, 20
    - Grabb for, 12–13
    - Nmap for, 7–9, 14
    - in perimeter defense, 122, 138
    - in wireless networks, 61
    - for worms, 93
  - IP checksum errors, 39
  - IPC\$ shares, 197
  - IPFilter tool, 252
  - IPSec, 144
  - iptables daemon, 115
  - IPTraf tool, 39
  - IRC (Internet Relay Chat) programs, 45–47
  - ITS (incident tracking system), 262
- J**
- Jacks for worm attacks, 103
- K**
- Key recovery process in PKI, 309
  - Keywords in evidence analysis, 253
  - Kismet scanner, 57–59, 61
  - KLINE command, 47
- L**
- LAN monitors, 39
  - Landscapers case. *See* Cyber extortion incident
  - LANs (local area networks), 4–5
  - Laptops
    - for configuration repositories, 156
    - for wireless networks, 57–58, 60–61
    - for worm attacks, 103
  - LEAP protocol, 61, 63–64, 67
  - Legal concepts and issues
    - chain of custody, 259–262
    - in disaster incident, 160
    - evidence guidelines, 262–263
    - for security policies, 167
  - Lessons learned
    - cyber extortion, 305
    - disaster incident, 162–163
    - DoS attacks, 47–49
    - executive fraud, 279–280
    - home architecture, 33–36
    - industrial espionage, 255
    - perimeter defense, 140–141
    - site defacement, 113–116
    - social engineering, 232–234
    - target networks, 21–22
    - virus attacks, 79–81
    - war-dialing attacks, 216–220
    - worms, 99–103
  - Liability issues, 160
  - License clauses, 258
  - License losses from worm attacks, 98
  - Linux laptops for wireless networks, 57–58
  - Load balancers, 49
  - Load sets, 152
  - LoadRunner tool, 133
  - Local area networks (LANs), 4–5
  - Local governments, worm incident. *See* Worm attacks
  - Locks for evidence, 271–272
  - Log File option in TextSearch Plus, 303–304

- Log ins
  - with single sign-on, 313–314
  - in war dialing, 211
- Log-on IDs, changing, 287
- Logical connections, 5–6
- Logical file structures, 275–277
- Logs
  - for evidence, 254, 260, 262
  - for HIPAA, 195, 201
  - in home architecture incident, 26–27, 32–34
  - for remote-access attempts, 219
  - in site defacement incident, 115
  - in virus attacks, 70–71, 75, 77–78
  - in war dialing, 219
  - for worms, 87, 99
- LOphtCrack tool, 57
- Losses
  - from DoS attacks, 44
  - from social engineering, 231–232
  - from virus attacks, 77–79
  - from worm attacks, 96–98
- Lovsan worm, 89
- Low-tech paths. *See* Social engineering
  
- M**
- M option, 14
- MAC (media access control), 65–67
- Machine losses from worm attacks, 98
- Maintenance windows in home architecture incident, 34
- Management in security policy development
  - questions for, 177–178
  - reviews by, 173
- Managers in ESM, 198
  
- Masking tape
  - in cyber extortion incident, 287
  - in industrial espionage incident, 242
- Master servers, 45
- Material for security policies, 172
- max\_parallelism option, 14
- Maximum downtime, 159
- MD5 checksums and digests, 248, 275, 294–300
- md5sum utility, 275
- Media access control (MAC), 65–67
- Medical clinic case. *See* Health Insurance Portability and Accountability Act (HIPAA)
- Medical research firm virus incident, 69–72
  - damage assessment, 77–79
  - lessons learned, 79–81
  - sources of, 72–77
- Memory cards, 242
- Military, wireless networks for, 55
- Minimum secure baselines in virus attacks, 80
- Mirroring
  - data, 162
  - hard drives, 243, 247, 290, 293
- Modems
  - access restrictions to, 216–218
  - rogue, 196, 208, 220
  - war dialing. *See* War-dialing attacks
- Monitoring
  - wireless networks, 66
  - for worm attacks, 99–100
- Monthly bills in home architecture incident, 26–27
- Mortgage services company incident. *See* Disaster incident

INDEX

---

- Motion detectors, 272
- MS Blaster worm, 89
- MS RPC bug, 89
- Multifactor authentication, 217–218
- Multiple data centers in worm incident, 84–85
- Multiple Matches option in TextSearch Plus, 304
- Mysqld daemon, 106–107
  
- N**
- NAT (NetBIOS Auditing Tool), 197
- NAT (Network Address Translation), 122
- National Infrastructure Protection Center (NIPC), 202–203
- National Institute of Standards and Technology (NIST), 123, 171
- Nessus scanner, 194
- net commands, 197, 244
- NetBIOS Auditing Tool (NAT), 197
- NetBus Trojan horse, 281–283
- netcat tool, 12
- NetStumbler tool, 58–59
- Network Address Translation (NAT), 122
- Network-based IDS (NIDS)
  - for perimeter defense, 134
  - for virus attacks, 72
- Network cable acquisition, 245
- Network configurations, repositories for, 156
- Network jacks, 103
- Network segmentation, 35
- Network-sniffing utilities
  - for DoS attacks, 39
  - Web site for, 50
- Network usage reports, 26–27
- Networks
  - in evidence acquisition, 243
  - target. *See* Target networks
  - VPNs. *See* Virtual private networks (VPNs)
  - wireless. *See* Wireless networks
  - in worm incident, 84–85
- NIDS (network-based IDS)
  - for perimeter defense, 134
  - for virus attacks, 72
- NIPC (National Infrastructure Protection Center), 202–203
- NIST (National Institute of Standards and Technology), 123, 171
- Nmap\_services file, 14
- Nmap tool
  - hiding, 19–21
  - for network architecture, 3–7
  - for OS identification, 13–16
  - for port scans, 7–13
  - reference for, 322
  - for site defacement assessment, 106
- Noise in war dialing, 211
- Nondisclosure agreements, 239, 258
- Normal files
  - in cyber extortion incident, 301
  - in industrial espionage incident, 252
- Normal timing policy, 20
- Notification procedures, 155
- NTFS file system, 247, 293
- Null connections, 197
- Null passwords, 198
- Null sessions, 197
- Number masquerading, 215

**O**

- O command, 13
- Off-site storage, 157–158
- oN flag, 14
- Online banking. *See* Perimeter defense;  
Wireless networks
- Online trading sites incident. *See* Social  
engineering
- Open Shortest Path First (OSPF)  
information, 39
- Operating systems
  - differences in, 199
  - identifying, 13–16
  - port scans for, 11
  - in site defacement assessment, 106
  - in war dialing, 212
- Optimization in war dialing, 210
- Options menu in TextSearch Plus, 303
- Orientation sessions for security  
policies, 185
- OSPF (Open Shortest Path First)  
information, 39
- Outbound blocks for worms, 92–94
- OverSeas Financial Services company.  
*See* Perimeter defense
- Owned machines in virus attacks, 71

**P**

- P0 flag, 12, 14
- packet\_trace option, 18
- packetstormsecurity.org site, 108
- Paper-based processes for worm  
attacks, 100
- Parallel port cable acquisition, 245
- Paranoid timing policy, 20
- Partition analysis, 246, 292
- passprop.exe utility, 197
- Passwords, 198
  - automated processes for, 232–233
  - changing, 287
  - cracking, 197
  - in HIPAA tests, 201
  - in home architecture incident, 34
  - in identity management, 311–312
  - insecure, 196
  - for modem access, 209
  - with NetBus, 282
  - operating system differences in, 199
  - policies for, 172, 181
  - in single sign-on, 313–314
  - in site defacement assessment,  
109–110, 112
  - social engineering of, 223, 227–230
  - in war dialing, 209, 211–212
  - in wireless networks, 57, 65
- Patches
  - for DoS attacks, 47
  - for HIPAA, 195
  - for virus attacks, 71–72, 75, 77
- Patient records. *See* Health Insurance  
Portability and Accountability Act  
(HIPAA)
- PDA's (personal digital assistants)
  - in HIPAA tests, 201
  - in worm attacks, 103
- Peer reviews of security policies, 173
- Penetration tests for HIPAA, 196
- Performance in perimeter defense  
research, 125–126, 130

INDEX

---

- Perimeter defense, 119
  - background, 119–121
  - company description, 121–123
  - implementation follow-up, 134–140
  - lessons learned, 140–141
  - market research, 129–131
  - pilot testing, 131–134
  - production networks for, 134
  - requirements, 123–129
- Permissions in site defacement
  - assessment, 111
- Person or Entry Authentication
  - standard, 190
- Personal digital assistants (PDAs)
  - in HIPAA tests, 201
  - in worm attacks, 103
- Personally identifiable information, 182
- PHI (protected health information).
  - See* Health Insurance Portability and Accountability Act (HIPAA)
- Phone dialing attacks. *See* War-dialing attacks
- PhoneSweep tool, 196
- Physical safeguards in HIPAA, 190
- Pictures for evidence
  - in cyber extortion incident, 287, 306
  - in executive fraud incident, 272
  - in industrial espionage incident, 242, 259
- Pilot groups for security policy reviews, 183
- Pilot testing of perimeter defense, 131–134
  - ping utility, 40
- PKI (public key infrastructure), 308–310, 325
- Points in perimeter defense research
  - scoring, 131, 133
- Policies
  - in PKI, 309
  - security. *See* Security policies
- Polite timing policy, 20
- Polymorphic worms, 83, 96
- POP3 port scans, 11
- Port lists, site for, 137
- Ports
  - number assignments for, 306
  - scanning, 7–13
- Positive control in executive fraud
  - incident, 271
- Power settings in wireless networks, 64, 67
- Pressing charges, 284–288
- Privacy
  - e-mail, 258
  - medical records. *See* Health Insurance Portability and Accountability Act (HIPAA)
- Private information, 182
- Proactive actions for wireless networks, 54
- Probative evidence, 262
- Procedures in security policies, 172–173
- Processes in virus attacks, 70
- Processing capacity for DoS attacks, 49
- Product users in perimeter defense
  - research, 129
- Production networks for perimeter defense, 134
- Productivity losses
  - from downtime, 159
  - from worm attacks, 97
- Professional reputation losses, 44
- Proprietary research. *See* Industrial espionage incident



- Protected health information (PHI). *See*  
Health Insurance Portability and  
Accountability Act (HIPAA)
- Proxy firewalls, 18–19
- PTable tool  
in evidence acquisition, 246–247, 292  
in evidence authentication, 251, 300
- Public information, 182
- Public intellectual assets, 256
- Public key infrastructure (PKI), 308–310,  
325
- Public relations  
in disaster incident, 151, 160–161  
in home architecture incident, 33
- Public trust losses, 98
- Publishing security policies, 173–174
- Q**
- Q&A sessions for security policies, 185
- Quality reviews of security policies, 173
- Questions in security policy development,  
177–178
- R**
- Radar-based motion detectors, 272
- RADIUS (Remote Authentication Dial-In  
User Service) authentication  
for financial transactions, 144  
in war dialing, 218
- Random dialing in war dialing, 210,  
214–215
- Random number generator, 269
- randomize\_hosts flag, 14
- Raw data files, 275
- Real estate company incident. *See* Disaster  
incident
- Real evidence, 262
- Rebooting  
in evidence acquisition, 245  
in virus attacks, 70, 76
- Rebuilding machines, 96
- Recorders  
for evidence protection, 272  
in industrial espionage incident, 242
- Recording data for perimeter defense, 135
- redhat.com site, 108
- Regulations, HIPAA. *See* Health Insurance  
Portability and Accountability Act  
(HIPAA)
- Related alerts, 135–136
- Reliability of backups, 178
- Remote-access attempt logs, 219
- Remote Authentication Dial-In User  
Service (RADIUS) authentication  
for financial transactions, 144  
in war dialing, 218
- Reporting  
in executive fraud incident, 278–279  
in perimeter defense, 127–128  
for worm attacks, 99–100
- Repositories for network configurations,  
156
- Reputation losses, 44
- Requests for Comments (RFCs), 13
- Research  
for perimeter defense, 135, 137  
for security policies, 171  
for social engineering, 224

INDEX

---

- Research firm virus incident, 69–72
    - damage assessment, 77–79
    - lessons learned, 79–81
    - sources of, 72–77
  - Research In Motion (RIM) devices, 55
  - Resistance to change, 54
  - Restoration of business functions, 150
  - RESTORE process, 244
  - Restrict Anonymous registry key, 197
  - Retention, e-mail, 258
  - Retina Network Security Scanner tool, 95
  - Retinal scans, 218
  - Retrofitting for wireless networks, 54
  - Return on investment (ROI)
    - for perimeter defense, 138–140
    - from single sign-on, 313–315
    - for wireless networks, 54
  - Review process for security policies, 173–174, 183
  - RFCs (Requests for Comments), 13
  - RFmon tool, 39
  - .rhosts file, 76
  - RIM (Research In Motion) devices, 55
  - Risk analysis and assessment, 148
    - in disaster incident, 158–159
    - in HIPAA, 191, 201–202
  - Road MASter analysis system, 245, 306
  - Rogue modems, 196, 208, 220
  - ROI (return on investment)
    - for perimeter defense, 138–140
    - from single sign-on, 313–315
    - for wireless networks, 54
  - Roles in PKI, 308
  - Root kits, 44
  - Root permissions, 111
  - Route-tracing tools, 17–18
  - Routers for HIPAA, 194–195
  - rsc command, 19
  - Rules
    - for HIPAA, 194
    - for perimeter defense, 138
    - for virus attacks, 72–74
  - Runaway processes, 70
- S**
- sadmind/IIS worm, 70–71, 76, 78
  - Safety, downtime effects on, 159
  - Salvaging operations, 150–151
  - SamSpade tool, 193
  - SANS Institute, 171
  - Sarbanes-Oxley Act, 188
  - Savings from IDSs, 139
  - Scalability in PKI, 309–310
  - Scan hosts, 138
  - Scans
    - hiding, 19–21
    - port, 7–13
  - Scores in perimeter defense research, 130–131, 133
  - Screen savers, biometrics for, 315
  - Scripts, hacking, 221
  - Search menu in TextSearch Plus, 303
  - Searches
    - in cyber extortion incident, 301–304
    - in evidence analysis, 253
    - in executive fraud incident, 270, 277
    - Federal guidelines for, 262
  - Secret assets, 257
  - Secure architecture, 316, 322
  - Secure Shell (SSH) service, 106–107
  - SecurID authentication, 218

- Securing equipment
  - in evidence acquisition, 243, 289
  - in industrial espionage incident, 240
- Security Awareness and Training
  - standard, 189
- Security awareness sessions, 184
- Security Incident Procedures standard, 189
- Security Management Process
  - standard, 189
- Security officer positions for HIPAA, 203
- Security policies, 165–167
  - awareness of, 185–186
  - company background, 174–176
  - implementing, 184–185
  - initial writing, 181–183
  - interviews for, 177–180
  - kickoff for, 169
  - meetings for, 176–177
  - in PKI, 309
  - process, 168
  - publishing, 173–174
  - resources for, 171, 323
  - reviewing, 173–174, 183
  - starting points, 169–171
  - teamwork for, 168–169
  - updating, 174
  - writing process, 172–173
- Segmentation faults, 108
- Seizing computers, 262
- Sensitive data, 182, 257. *See also* Industrial espionage incident
- Serial Number List (SNL) tool, 198
- Servers
  - in DoS attacks, 45
  - identifying, 106
- Service-level agreements (SLAs), 149
- Service set identifiers (SSIDs)
  - names for, 58–60
  - in wireless networks, 61, 67
- Short-term recovery strategies, 161
- Shutting down computers, 243, 288–289
- sI flag, 20
- Signatures for worms, 92, 95
- Simulated attacks, 133
- Single sign-on (SSO), 312–315
- Site defacement incident, 105–106
  - damage assessment, 106–113
  - lessons learned, 113–116
- Slack
  - in cyber extortion incident, 301
  - in executive fraud incident, 277
  - in industrial espionage incident, 252
- SLAs (service-level agreements), 149
- SMTP port scans, 11–12
- Sneaky timing policy, 20
- SNL (Serial Number List) tool, 198
- snlist tool, 198
- Snort tool
  - for DoS attacks, 39, 48
  - for financial transactions, 144
  - resource for, 137
- Social engineering, 221–223
  - damage from, 231–232
  - exit strategies, 231
  - lessons learned, 232–234
  - preparation, 224–225
  - process, 225–230
  - resources for, 324
- Social Security numbers, 229–230
- Sockets, maximum number of, 14
- Software license clauses, 258
- Software license losses, 98

INDEX

---

- Source IP addresses, 138
  - Source phone numbers in war dialing, 217
  - Special Publication 800–31, 123
  - Spoofed IP addresses, 42
  - Spying. *See* Industrial espionage incident
  - SSH (Secure Shell) service, 106–107
  - sshd daemon, 106, 108
  - SSIDs (service set identifiers)
    - names for, 58–60
    - in wireless networks, 61, 67
  - SSL for financial transactions, 144
  - SSO (single sign-on), 312–315
  - Standards
    - for HIPAA, 202–203
    - in security policies, 172–173
  - Starting points for security policies, 169–171
  - State governments, worms in. *See* Worm attacks
  - Static electricity, 242, 287
  - Stock-trading sites incident. *See* Social engineering
  - Stories in social engineering, 226–227
  - Stovepipe setup and worms, 83–84
  - String searches, 277
  - Strong authentication, 65
    - sU flag, 10
  - Suspect systems, 267–268
    - sV flag, 7
  - Swapping hard drives, 300
    - sX flag, 17
  - SYN packets
    - in DoS attacks, 42
    - for firewall detection, 19
    - for port scans, 13
  - Synchronizing user credentials, 312
  - syslog service, 115
  - System administrator questions in policy development, 177
  - System backups for worm attacks, 99
  - System date and time in evidence
    - acquisition, 245–246, 291–292
  - System Scanner tool, 95
- T**
- T flag, 20
  - TACACS (Terminal Access Controller Access Control System), 218
  - Tape backup cartridges, 287
  - Tape drive acquisition, 245, 293
  - TAPI (Telephony Application Programming Interface)
    - standard, 211
  - Target networks, 3
    - architecture, 3–7
    - hiding scans of, 19–21
    - lessons learned, 21–22
    - OS identification, 13–16
    - partial picture of, 17–19
    - port scans of, 7–13
  - Task forces for worms, 90–91
  - TCP (Transmission Control Protocol)
    - port scans, 10
    - three-way handshakes, 42
    - traffic monitoring, 39
  - TCP/IP boot disks, 244
  - Tcpdump tool, 18
    - for DoS attacks, 39–40
    - Web site for, 50
  - Teamwork for security policies, 168–169
  - Technical safeguards in HIPAA, 190

- Telecommuting, security policies for, 184
  - Telephone dialing. *See* War-dialing attacks
  - Telephone support, social engineering of, 227–230
  - Telephony Application Programming Interface (TAPI) standard, 211
  - Telnet, 11–12
  - Templates for security policies, 172, 181
  - Temporary workspace in disaster incident, 151
  - Terminal Access Controller Access Control System (TACACS), 218
  - Termination process, intellectual asset protection in, 256
  - Testing
    - perimeter defense, 131–134, 140
    - wireless networks, 56
  - Texas Department of Information site, 171
  - TextSearch Plus tool, 252–253, 301–304
  - Three-way handshakes, 42
  - Time documentation, 245–246, 291–292
  - Time losses from worm attacks, 97
  - Time to Live (TTL) value, 18
  - Timeout settings in war dialing, 210
  - Timing options in Nmap, 20
  - Tokens in authentication, 218
  - Top secret assets, 257
  - Traceroute tool, 17
  - Tracking surfing habits, 208
  - Trade secrets clauses, 257
  - Trading sites incident. *See* Social engineering
  - Traffic filtering
    - for DoS attacks, 47–48
    - Web site for, 50
    - in wireless networks, 65–66
  - Training for perimeter defense, 134–135
  - Transactions, online trading sites. *See* Social engineering
  - Transmission Control Protocol (TCP)
    - port scans, 10
    - three-way handshakes, 42
    - traffic monitoring, 39
  - Transmission Security standard, 190
  - Trends, 319
  - Tried-and-true targets, 207
  - Trojan horses, 281–283
  - TTL (Time to Live) value, 18
  - Two-factor authentication schemes, 218
- ## U
- UDP (User Datagram Protocol)
    - port scans with, 10
    - traffic monitoring, 39
  - Unallocated space
    - in cyber extortion incident, 301
    - in executive fraud incident, 277
    - in industrial espionage incident, 252
  - Unauthorized modems, 208
  - University site defacement incident, 105–106
    - damage assessment, 106–113
    - lessons learned, 113–116
  - UNIX operating system, 11
  - Unsolicited electronic mail, 258
  - Updating security policies, 174
  - urandom random number generator, 269
  - User Datagram Protocol (UDP)
    - port scans with, 10
    - traffic monitoring, 39

**INDEX**

---

- User names and accounts
    - in home architecture incident, 34
    - identity management for, 311
    - in site defacement assessment, 108–109
    - social engineering for, 225–226
    - in war dialing, 211
    - in wireless networks, 65
  - User privileges in war dialing, 218
  - User roles in PKI, 308
  - User settings, operating system differences
    - in, 199
  - userhelper program, 108
  - Userrooter script, 111
- V**
- v flags, 14
  - Vendors
    - controls on, 220
    - in perimeter defense research, 129
  - Verification step in social engineering, 233
  - Verifying data for perimeter defense, 135
  - VERITAS backup software, 144
  - Versions
    - daemon, 107–108
    - Nmap, 7
  - VFAT file system, 247, 293
  - VHS recorders for evidence protection, 272
  - Virtual local area networks (VLANs), 68
  - Virtual private networks (VPNs)
    - description, 316
    - for financial transactions, 144
    - in home architecture, 24–25, 29–30
    - resources for, 325
    - security policies for, 184
    - in virus attacks, 75, 79
  - Virus attacks, 69–72
    - damage assessment, 77–79
    - lessons learned, 79–81
    - resources for, 323
    - sources of, 72–77
    - worms. *See* Worm attacks
  - VisualRoute application, 17
  - VLANs (virtual local area networks), 68
  - VPNs. *See* Virtual private networks (VPNs)
  - Vulnerability analysis for HIPAA, 191
  - Vulnerability scanners, 194
- W**
- War-dialing attacks, 207–208
    - description, 208–209
    - lessons learned, 216–220
    - resources for, 324
    - techniques, 209–216
  - Warnings for security policies, 186
  - Web-based e-mail services in worm attacks, 102
  - Web security, resources for, 323
  - Web servers for HIPAA, 195
  - Web sites for security, 321–322
  - Weights in perimeter defense research scores, 131, 133
  - Well-known ports, 306
  - WEP (Wired Equivalent Privacy)
    - encryption, 55, 60, 62–63, 65–67
  - What's Running tool, 12
  - Whois tool, 9
  - Windows laptops for wireless networks, 57, 60–61
  - Windows of opportunity, 253
  - Windows operating system port scans, 11

- Wired Equivalent Privacy (WEP)
    - encryption, 55, 60, 62–63, 65–67
  - Wireless networks, 53–55
    - background, 55–56
    - end state, 66–68
    - existing security, 63–64
    - home systems, 318
    - project for, 57–63
    - recommendations for, 64–66
    - resources for, 322
  - Wireless scans, 66
  - Workforce Security standard, 189
  - Working at home, 317–318
  - Working backups, 243, 289
  - Workstation Security standard, 190
  - Workstation Use standard, 190
  - Worm attacks, 83–84
    - background, 84–85
    - contingency plans for, 100
    - corrective actions for, 100
    - diagnosis, 89
    - hot network jacks for, 103
    - infection by, 85–89
    - lessons learned, 99–103
    - losses from, 96–98
    - monitoring for, 99–100
    - plan of attack, 89–96
    - sadmind/IIS worm, 70–71, 76, 78
    - system backups for, 99
    - Web-based e-mail services in, 102
  - Writing security policies, 172–173
  - Writing skills, 165
  - www.securityfocus.com site, 108
- X**
- Xmas scans, 17–18
  - XPOT (Extended Phone Operations Tool), 209–210
  - xprobe tool, 15
- Z**
- Zcomax wireless cards, 58
  - Zombie hosts, 20–21
  - Zombies in DoS attacks, 41, 44–45
  - Zone transfers, 10–11

