

Index

- Abdallah, Abraham, 214
- access controls, vulnerability, 127
- accidents
- costs of damage, 54
 - role in espionage, 113
 - threats posed by, 53–54
- acts of God, 54–56
- administrator skills, vulnerability, 210
- agents. *See also* collectors; operatives
- definition, 5
 - desensitizing, 9–10
 - double, 6
 - mental weaknesses, 8–9
 - MICE (Money, Ideology, Coercion, Ego), 8–9
 - motivation, 8–9
 - recruiting, 8–10
 - special, 5–6
- agents, recruiting
- China, 86, 87
 - disgruntled employees, 62
 - espionage simulation, 162
 - France, 90
 - Israel, 93–94
 - mental weaknesses, 8–10
 - MICE (Money, Ideology, Coercion, Ego), 8–10
 - motivation, 8–10
 - typical case, 7
- airport hack, 147
- airports, espionage simulation
- attack, 183–185
 - case summary, 185–186
 - failure to check IDs, 184, 187–188
 - failure to motor vehicles, 185, 188
 - inconsistent security, 184, 187
 - observation areas, 188
 - physical controls, 183, 186
 - preparation, 182–183
 - reconnaissance, 181–182
 - security guards, 184, 187
 - sensitive information exposed, 188
 - tailgating, 183, 186
 - vulnerabilities exploited, 186–188
 - watching the obvious, 184, 186
- Al Qaeda, goals, 69
- alert failure, 210
- alert systems, 242–243
- Amazon.com fraud, 203–204
- analysis phase, 17–18
- anti-spyware software, 236
- anti-virus software, 227, 235, 279
- assessing risk. *See also* managing risk
- countermeasures factor, 33
 - overview, 32–33
 - threat factor, 33
 - value factor, 32
 - vulnerability factor, 33

- attackers. *See also* criminals; threat categories
 - collectors, 15, 67–68
 - phreakers, 75
- attackers, agents
 - definition, 5
 - desensitizing, 9–10
 - double, 6
 - mental weaknesses, 8–9
 - MICE (Money, Ideology, Coercion, Ego), 8–9
 - motivation, 8–9
 - recruiting, 8–10
 - special, 5–6
- attackers, hackers
 - Bavand, Afshin, 190–196
 - as consultants, 258–259
 - criminally inclined, 80
 - French, 92
 - Indian, 173–177
 - Israeli, 93
 - Russian, 85
 - technical expertise, 142
 - threats posed by, 74–75, 78–80
 - training, 252
- attackers, operatives
 - black bag operations, 10–11
 - definition, 6
 - NOC (non-official cover), 7
 - recruiting, 7
 - training, 7
- attackers, phishers
 - costs of damage, 59
 - description, 224–225
 - Internet schemes, 204–205
 - for passwords, 219
- attackers, spies
 - common perception, 4
 - risk management, 34
 - types of. *See* agents; collectors; operatives
- audit logs, 289–290
- auditing
 - cellular telephone networks, 199
 - computer use, 176–177, 179
 - automated patching, 285–286
 - availability, value, 46
 - awareness, vulnerability, 109–113
 - awareness training, 238–241
- background checks, 136–137, 261
- backups, 236, 281–283
- badges
 - acquiring, 172–173
 - espionage countermeasures, 246, 274–275
 - universal, 178
 - verification, 172–173, 178
- balancing point, risk management, 36–38
- bank fraud, costs of damage, 72
- banking information, loss of, 216
- Bavand, Afshin, 190–196
- bicycle shop, information value, 45
- black bag operations. *See also* espionage
 - definition, 10
 - espionage simulation, 158–160, 161–162
 - Iranian hostage crisis, 10
 - operatives performing, 10–11
- Black Ice*, 71
- Blaster worm, 141
- blogs, as information source, 26
- blueprints exposed, 175, 179
- BND (Bundesnachrichtendienst), 94
- books about spies
 - Black Ice*, 71
 - Corporate Espionage*, 240
 - Friendly Spies*, 91
- budgeting for risk management, 38–39.
 - See also* costs of damage; information, value
- buffer overflows, 141
- bugs (listening devices), 151, 290–291
- bugs (software errors)
 - Gorshkov, Vasily, 209–210
 - Ivanov, Alexey, 209–210
 - programming errors, 209–210
 - technical vulnerabilities, 140–143
 - Wall Street programming errors, 54

- buildings, placement of, 135
- Bundesnachrichtendienst (BND), 94
- Bush, George W., 109
- business continuity, 282
- business opportunities scams, 223–224

- cable locks, 271
- call backs, 243–244
- caller ID, verifying, 243–244
- car safety, risk management, 35
- card access locks, 275
- carelessness, 113
- case studies
 - See also* crime
 - See also* espionage simulation
 - See also* vulnerabilities
 - Chinese incident, 88
 - Citibank theft, 216
 - defensive measures. *See* countermeasures
 - E*Trade.com denial-of-service, 216
 - French espionage, 91
 - Good Morning America, 24
 - hazardous material transport, 66
 - “I Love You” virus, 112
 - information value, 45
 - Iranian hostage crisis, 10
 - laptop theft, 215
 - loss of sensitive banking data, 215
 - pizza delivery, 5
 - presidential visit to Iraq, 109
 - risk management, 35, 38–39
 - safe cars, 35
 - war dialing, 147
 - Windows 95 passwords, 141
 - Worcester Airport hack, 147
- case studies, cellular telephone networks
 - auditing, 199
 - case summary, 196–197
 - CD capacity, 199
 - centralized document storage, 199
 - finding a target, 193–196
 - hacker history, 191–193
 - hacker profile, 189–191
 - layoffs, 198
 - low morale, 198
 - severance assistance, 198
 - unlimited document access, 199
 - vulnerabilities exploited, 196–199
- case studies, credit card fraud
 - defending against, 48–49
 - Good Morning America, 24
- casinovega.com break-in, 205–207
- CD capacity, cellular telephone networks, 199
- cellular phone conversations, limiting, 254
- cellular telephone networks
 - auditing, 199
 - case summary, 189–191, 196–197
 - CD capacity, 199
 - centralized document storage, 199
 - finding a target, 193–196
 - hacker history, 191–193
 - hacker profile, 189–191
 - layoffs, 198
 - low morale, 198
 - severance assistance, 198
 - unlimited document access, 199
 - vulnerabilities exploited, 196–199
- centralized document storage, 199
- chain letters, 222–223
- challenging strangers
 - Fortune 500 company, 157, 161, 169–170
 - nuclear plant, 173
- Charney, Scott, 140
- chemical and biological attacks, risk management, 32
- chief information officers (CIOs), 47
- China, threats posed by, 85–90
- Chinese incident, 88
- CIOs (chief information officers), 47
- Citibank theft, 216
- classifying information, 241–242
- clean desk policies, 270
- Code Red worm, 141
- coercion, as motivation, 9
- collecting information. *See* black bag operations; espionage
- collection phase, 14–17
- Collection Requirements section, 84
- collectors, 15, 67–68. *See also* agents; operatives

- common sense, 110–111, 234
- competitors
 - espionage countermeasures, 248–249
 - information value, 48–49
 - threats posed by, 103–105
- computer access, espionage simulation, 159, 168
- computer auditing, 176–177, 179
- computer crime. *See also* crime, against individuals; crime, on the Internet
 - defensive strategies. *See* countermeasures phreakers, 75
 - viruses and worms, 141
- computer crime, hackers. *See also* criminals; spies; *specific names*
 - criminally inclined, 80
 - French, 92
 - Indian, 173–177
 - Israeli, 93
 - Russian, 85
 - technical expertise, 142
 - threats posed by, 74–75, 78–80
- computer crime, hacking computers
 - methods, 76–77
 - Worcester Airport, 147
- computer crime, phishing
 - costs of damage, 59
 - description, 224–225
 - Internet schemes, 204–205
 - for passwords, 219
- computer security, 175, 179
- computer-based information sources, 22–23
- computers not logged out, 133
- confidentiality, value, 44
- configuration baselines, 286–287
- configuration errors, 143–144
- construction procedures, espionage simulation, 159, 167
- consultants
 - checking, 267
 - hackers as, 258–259
 - skill levels, 211
 - threats posed by, 64–65
- contracted services, espionage countermeasures, 267–268
- contractual relationships, vulnerability, 125
- conversations
 - as information source, 27–28
 - outside work, limiting, 254
 - vulnerability, 119–120
- cookies, 117, 236–237
- cooking the books, 19
- copy machines, vulnerability, 129, 271–272
- cordless phone conversations, limiting, 254
- corporate culture, and security programs, 298
- Corporate Espionage*, 240
- corporate releases, reviewing, 247–248
- cost/risk relationship, 36–38
- costs of damage. *See also* budgeting; information, value
 - accidents, 54
 - background checks, 261
 - bank fraud, 72
 - to consumers, 216–217
 - earthquakes, 55
 - expense of security, 211–212
 - fires, 55
 - floods, 55
 - Hubble Space Telescope, 54
 - human error, 54
 - hurricanes, 55
 - insider attacks, 60, 62
 - laptop theft, 100
 - lightning, 55
 - NASA Mars probe, 54
 - phishers, 59
 - power outages, 55, 277–278
 - spam, 58
 - viruses and worms, 58–59
 - Wall Street programming errors, 54
- countermeasures
 - balancing with vulnerabilities, 36–38
 - choosing, 296–298
 - defense in depth, 304–305
 - factor in risk equations, 33
 - maximizing, 35
 - measuring success, 304
 - overview, 231–234
 - security programs, developing, 295–298
 - selection factors, 297

- countermeasures, all purpose
 - anti-spyware software, 236
 - anti-virus software, 235
 - backing up data, 236
 - common sense, 234
 - cookies, clearing, 236–237
 - disaster preparation, 237
 - firewalls, 235
 - history files, clearing, 236–237
 - Ira's Four Golden Rules, 235
 - limiting Internet postings, 234–236
 - log files, clearing, 236–237
 - system utilities, 237
 - temporary files, clearing, 236–237
- countermeasures, operational
 - awareness training, 238–241
 - badges, 246
 - call backs, 243–244
 - caller ID, verifying, 243–244
 - cellular phone conversations, limiting, 254
 - classifying information, 241–242
 - competitors, 248–249
 - conversations outside work, limiting, 254
 - cordless phone conversations, limiting, 254
 - disaster recovery, 256–257
 - employee morale, 239
 - giving advice, 239
 - guidelines for marketers and salespeople, 248
 - hacker training, 252
 - hackers as consultants, 258–259
 - ID, verifying, 244–245
 - incident handling, 256–257
 - information access, verifying need for, 244–245
 - Infraguard, 252–253
 - interdepartmental security, 255–256
 - Internet activity, monitoring, 249–250
 - minimizing data storage, 250
 - nondisclosure/noncompete agreements, 246–247
 - overview, 238
 - penetration testing, 259–260
 - phone conversations, limiting, 253–254
 - predictability, 255
 - Professional organizations, 252–253
 - reviewing corporate releases, 247–248
 - rewards, 243
 - security alert systems, 242–243
 - separate phone lines, 253
 - technical training, 251
 - technical vulnerabilities, monitoring, 250–251
 - vulnerability assessments, 257, 259–260
- countermeasures, personnel
 - background checks, 261
 - employee hotlines, 262
 - employee roles, establishing, 265–266
 - employees, categorizing, 265–266
 - HR, coordinating with IS, 262–263
 - HR, coordinating with security department, 263–264
 - information access, tracking, 264
 - overview, 260–261
 - requirements on contracted services, 267–268
 - security professionals, checking, 267
 - spouse checks, 262
 - terminations, coordinating, 266–267
 - visitors, reviewing, 264–265
- countermeasures, physical
 - badges, 274–275
 - cable locks, 271
 - card access locks, 275
 - choosing a location, 276
 - clean desk policies, 270
 - copy machine controls, 271–272
 - dumpster locks, 273
 - facility walk-throughs, 270
 - fire suppression, 277
 - guard training, 275–276
 - information locks, 268–269
 - library control, 272
 - off-site business, 277
 - overview, 268
 - password protection, 269
 - perimeter locks, 274
 - recycle bins, 273
 - removal of equipment, 274
 - screen savers, 269

- countermeasures, physical (*Continued*)
 - security patrols, 276
 - security reminders, 272
 - shredders, 272–273
 - strange postings, 270–271
 - unusual access, 274
 - UPSs (uninterruptible power supplies), 277–278
- countermeasures, technical
 - anti-virus software, 279
 - audit logs, 289–290
 - automated patching, 285–286
 - backups, 281–283
 - bug sweeps, 290–291
 - business continuity, 282
 - configuration baselines, 286–287
 - disaster recovery, 282
 - encryption, 291–292
 - firewalls, 279–280
 - intrusion detection/prevention, 280–281
 - mirrored logs, 290
 - multifactor authentication, 287–288
 - off-line data storage, 292
 - overview, 278
 - single sign-on software, 288
 - software testing, 286
 - vulnerability scanners, 283
 - war dialing, 283–284
 - wireless security, 284–285
 - wiretap sweeps, 290–291
- countries, threats posed by
 - China, 85–90
 - Cuba, 99–100
 - France, 90–92
 - Germany, 94–95
 - India, 97–98
 - Iran, 98–99
 - Israel, 93–94
 - Japan, 95–97
 - overview, 80–81
 - Russia, 81–85
- crackers, threats posed by, 75
- credit card fraud. *See also* identity theft
 - crime against individuals, 221–222
 - defending against, 48–49
 - Good Morning America, 24
 - Gorshkov, Vasily, 206–207
 - organized crime, 73
 - perpetrators, 57–58
 - theft of numbers, 215
- credit cards, vulnerability, 119
- crime
 - examples of. *See* case studies
 - organized, 71–74, 82
 - petty, 100–101
 - simulating. *See* espionage simulation
 - types of. *See* threat categories
 - vulnerability to. *See* vulnerabilities
- crime, against individuals
 - antivirus software, 227
 - banking information, 216
 - business opportunities, 223–224
 - chain letters, 222–223
 - credit card fraud, 221–222
 - credit card theft, 215
 - denial-of-service attacks, 226
 - eBay fraud, 218–219
 - in the future, 225
 - greed, 227
 - healthcare, 224
 - Internet access services, 219
 - Internet auctions, 218–219
 - Internet kiosks, 223–224
 - investments, 220–221
 - “Make money fast” schemes, 223–224
 - malicious software, 225–226
 - modem highjacking, 221
 - most likely threats, 217–226
 - multilevel marketing, 222–223
 - phishing, 219, 224–225
 - pornography, 221
 - pyramid schemes, 222–223
 - security awareness, 227
 - spyware, 225–226
 - stock tips, 220–221
 - travel scams, 220
 - vacation scams, 220
 - vulnerabilities exploited, 226–227
 - web cramming, 220
 - work-at-home schemes, 223–224
 - zombie software, 226

- crime, on the Internet
 - administrator skills, 210
 - alert failure, 210
 - Amazon.com fraud, 203–204
 - case summary, 208–209
 - casinovega.com break-in, 205–207
 - credit card fraud, 206–207
 - criminal background, 202–204
 - culture relations, 212–213
 - eBay fraud, 203–204
 - extortion, 206–207
 - front organizations, 204–205
 - getting caught, 207
 - international relations, 212–213
 - Lightrealm attack, 205–206
 - making of a criminal, 201–202
 - password exposures, 213
 - PayPal fraud, 204
 - perceived expense of security, 211–212
 - phishing schemes, 204–205
 - programming errors, 209–210
 - restitution, 209
 - security awareness, 212
 - security consultant skills, 211
 - undetected compromises, 210
 - unnecessary data, 212
 - vulnerabilities exploited, 209
 - web-hosting break-ins, 205–207
- criminals, threats posed by. *See also* attackers
 - credit card fraudsters, 57–58
 - identity thieves, 56–57
 - malware, 59–60
 - phishers, 59
 - spammers, 58
 - spyware, 59–60
 - viruses and worms, 58–59
- crying wolf, 303
- Cuba, threats posed by, 99–100
- culture relations, vulnerability, 212–213
- customers, threats posed by, 102
- cyber cartels, 73
- cyberterrorism, 70–71

- damage costs. *See* costs of damage
- data flow analysis, 18
- data storage, minimizing, 250

- data transmission, vulnerability, 147–148
- death by 1,000 cuts, 40. *See also*
 - information, value
- defense in depth, 304–305
- defense strategies
 - See* case studies
 - See* countermeasures
 - See* security programs
 - See* vulnerabilities
- denial-of-service attacks, 60, 73, 226
- departing workers, threats posed by, 63
- desensitizing agents, 9–10
- DGSE (French intelligence)
 - industrial espionage, 90
 - infiltrating American firms, 16
- Dick, Ron, 52
- disaster recovery, 237, 256–257, 282
- disgruntled employees, threats posed by, 62–63
- disinformation, 16–17
- documents
 - centralized storage, 199
 - as information source, 23–24
 - unlimited access, 199
- double agents, 6
- draft documents, as information source, 23–24
- dumpster locks, 273

- earthquakes, 55
- eBay fraud, 203–204, 218–219
- ego, as motivation, 9
- electrical systems, vulnerability, 134–135
- electromagnetic pulses (EMPs), 150
- electronic storage, vulnerability, 129
- e-mail
 - addresses, value, 43
 - as information source, 22–23
- employees. *See also* insiders; personnel
 - categorizing, 265–266
 - disgruntled, threats posed by, 62–63
 - former, threats posed by, 63–64
 - hotlines, 262
 - morale, 198, 239
 - on-site nonemployees, 64–65
 - roles, establishing, 265–266
 - threats posed by, 60–62

- EMPs (electromagnetic pulses), 150
- encryption, 291–292
- entrepreneur. *See* cellular telephone networks
- environment, vulnerability, 130–131
- equation, risk assessment
 - countermeasures factor, 33
 - overview, 32–33
 - threat factor, 33
 - value factor, 32
 - vulnerability factor, 33
- equipment, placement of, 135
- equipment size, vulnerability, 131–132
- Ericsson hack. *See* cellular telephone networks
- errors and omissions, 113
- escorts, lack of, 167–168
- espionage. *See also* case studies; industrial espionage; vulnerabilities
 - defensive measures. *See* countermeasures
 - perfect crime, 4
 - prime rule, 3
- espionage simulation, airports
 - attack, 183–185
 - case summary, 185–186
 - failure to check IDs, 184, 187–188
 - failure to motor vehicles, 185, 188
 - inconsistent security, 184, 187
 - observation areas, 188
 - physical controls, 183, 186
 - preparation, 182–183
 - reconnaissance, 181–182
 - security guards, 184, 187
 - sensitive information exposed, 188
 - tailgating, 183, 186
 - vulnerabilities exploited, 186–188
 - watching the obvious, 184, 186
- espionage simulation, Fortune 500
 - company
 - black bag operation, 158–160, 161–162
 - case summary, 165–166
 - computer access, 159, 168
 - construction procedures, 159, 167
 - labeling computers, 159
 - lack of escorts, 167–168
 - mission description, 156–158
 - mission execution, 162–166
 - no challenge to strangers, 157, 161, 169–170
 - perimeter security, 157–158, 160, 166
 - reporting procedures, 169
 - security awareness, 169
 - security guards, 157, 161, 163, 166–167
 - social engineering, 160–161
 - social security numbers as IDs, 160, 169
 - tailgating, 158, 170
 - telecommunications access, 168–169
 - vulnerabilities exploited, 166–170
- espionage simulation, nuclear power plant
 - acquiring badges, 172–173
 - badge verification, 172–173, 178
 - blueprints exposed, 175, 179
 - case summary, 177
 - computer auditing, 176–177, 179
 - computer security, 175, 179
 - ID verification, 172, 177–178
 - labeling computers, 176, 179
 - locks, 172, 178
 - security guards, 173
 - social engineering, 172–176
 - tailgating, 173
 - unauthorized penetration, 173–177
 - universal badges, 178
 - vulnerabilities exploited, 177–179
- E*Trade.com denial-of-service, 216
- evaluation phase
 - cooking the books, 19
 - definition, 19–20
 - determining value, 20
 - purpose, 19–20
 - tampering with results, 19
- examples. *See* case studies
- extortion, 206–207
- facility walk-throughs, 270
- fire suppression, 277
- fires, 55
- firewalls, 146–147, 235, 279–280
- firing employees
 - coordinating terminations, 266–267
 - separation procedures, 138

- severance assistance, 198
- vulnerabilities, 138
- floods, 55
- formal documents, as information
 - source, 23
- formal meetings, as information source, 27
- former employees, threats posed by, 63–64
- Fortune 500 company, espionage simulation
 - black bag operation, 158–160, 161–162
 - case summary, 165–166
 - computer access, 159, 168
 - construction procedures, 159, 167
 - labeling computers, 159
 - lack of escorts, 167–168
 - mission description, 156–158
 - mission execution, 162–166
 - no challenge to strangers, 157, 161, 169–170
 - perimeter security, 157–158, 160, 166
 - reporting procedures, 169
 - security awareness, 169
 - security guards, 157, 161, 163, 166–167
 - social engineering, 160–161
 - social security numbers as IDs, 160, 169
 - tailgating, 158, 170
 - telecommunications access, 168–169
 - vulnerabilities exploited, 166–170
- Four Golden Rules, 235
- France, threats posed by, 90–92
- French espionage example, 91
- French intelligence (DGSE)
 - industrial espionage, 90
 - infiltrating American firms, 16
- Friendly Spies*, 91
- front organizations, 204–205
- garbage, vulnerability, 127–128
- gas masks, risk management, 32
- Germany, threats posed by, 94–95
- Golden Rules, 235
- Golovkin, Sergei, 194
- Good Morning America, 24
- googling, 26, 118
- Gorshkov, Vasily
 - administrator skills, 210
 - alert failure, 210
- Amazon.com fraud, 203–204
- background, 202–204
- case summary, 208–209
- casinovega.com break-in, 205–207
- credit card fraud, 206–207
- culture relations, 212–213
- eBay fraud, 203–204
- extortion, 206–207
- front organizations, 204–205
- getting caught, 207
- international relations, 212–213
- Lightrealm attack, 205–206
- making of, 201–202
- password exposures, 213
- PayPal fraud, 204
- perceived expense of security, 211–212
- phishing schemes, 204–205
- programming errors, 209–210
- restitution, 209
- security awareness, 212
- security consultant skills, 211
- undetected compromises, 210
- unnecessary data, 212
- vulnerabilities exploited, 209
- web-hosting break-ins, 205–207
- greed, and crime, 227
- guidelines for marketers and salespeople, 248
- hackers. *See also* criminals; spies; *specific names*
 - Bavand, Afshin, 190–196
 - as consultants, 258–259
 - criminally inclined, 80
 - French, 92
 - Indian, 173–177
 - Israeli, 93
 - Russian, 85
 - technical expertise, 142
 - threats posed by, 74–75, 78–80
 - training, 252
- hacking computers. *See also* viruses and worms
 - methods, 76–77
 - Worcester Airport, 147
- Hale, Larry, 108

- hazardous material transport, 66
- healthcare, vulnerability, 224
- help wanted ads, vulnerability, 117
- hidden information value, 43–48
- history files, clearing, 236–237
- homeland security, and security programs, 302–304
- hotlines, 262
- HR department, coordinating with
 - IS, 262–263
 - security department, 263–264
- Hubble Space Telescope, costs of damage, 54
- human error, 53–54
- Human Intelligence (HUMINT), 15
- Human Resources, coordinating with
 - IS, 262–263
 - security department, 263–264
- human resources, vulnerability, 138–139
- human weakness, vulnerability, 123–124
- HUMINT (Human Intelligence), 15
- hurricanes, 55

- “I Love You” virus, 112
- IBM salespeople, 101–102
- identity theft, 56–57. *See also* credit card fraud
- ideology, as motivation, 8
- IDs
 - caller, verifying, 243–244
 - failure to check, 184, 187–188
 - failure to check, airports, 184, 187–188
 - social security numbers as, 160, 169
 - verifying, 172, 177–178, 244–245
 - verifying, countermeasure, 244–245
 - verifying, nuclear power plant, 172, 177–178
- Imagery Intelligence (IMINT), 15
- IMINT (Imagery Intelligence), 15
- inboxes, vulnerability, 132–133
- incident handling, 256–257
- India, threats posed by, 97–98
- industrial espionage. *See also* countries, threats posed by; espionage; espionage simulation
 - DGSE (French intelligence), 90
 - information value, 48–49
 - Industry Structure section, 83
 - informal meetings, as information source, 27
- information. *See also* intelligence
 - access, tracking, 264
 - access, verifying need for, 244–245
 - classifying, 241–242
 - collecting. *See* espionage
 - disinformation, 16–17
 - espionage countermeasures, 241–242
 - importance of form, 21–22
 - locks, 268–269
 - seeding, 17
- information, collection
 - from businesses. *See* industrial espionage
 - directly from the source. *See* black bag operations
 - methods, 16
- information, forms of
 - blogs, 26
 - casual conversations, 27–28
 - computer based, 22–23
 - draft documents, 23–24
 - e-mail, 22–23
 - formal documents, 23
 - formal meetings, 27
 - googling, 26
 - informal meetings, 27
 - internal correspondence, 25
 - legal filings, 25
 - miscellaneous records, 25–26
 - the press, 26
 - regulatory filings, 25
 - scrap paper, 24
 - working papers, 24
- information, value. *See also* budgeting; costs
 - of damage; evaluation phase
 - to adversaries and competitors, 48–49
 - availability, 46
 - calculating, 49–50
 - confidentiality, 44
 - e-mail addresses, 43
 - hidden, 43–48
 - integrity, 45–46
 - monetary, 42–43

- nuisance value, 46–48
 - perceived, 41
 - physical assets, 42–43
- information is information, 21–22
- information resource management (IRM), 47
- information warriors, threats posed by, 66–67
- Infraguard, 252–253
- insiders, costs of damage, 60, 62. *See also* employees; personnel
- insiders, threats posed by
 - consultants, 64–65
 - departing workers, 63
 - disgruntled employees, 62–63
 - employees, 60–62
 - former employees, 63–64
 - offshoring, 65
 - on-site nonemployees, 64–65
 - outsourcing, 65
 - temporary workers, 64–65
 - thrill seekers, 63
- integrity, value, 45–46
- intelligence. *See also* information collectors, 15
 - HUMINT (Human Intelligence), 15
 - IMINT (Imagery Intelligence), 15
 - OSINT (Open Source Intelligence), 15
 - SIGINT (Signals Intelligence), 15
 - TRASHINT, 15
 - types of, 15
- intelligence process
 - common scenarios, 20–21
 - overview, 11–12
- intelligence process, phases
 - analysis, 17–18
 - collection, 14–17
 - evaluation, 19–20
 - requirements definition, 12–14
 - standard analysis, 18
 - traffic analysis, 18
- interdepartmental security, 255–256
- internal correspondence, as information source, 25
- international relations, 212–213
- Internet
 - access services, vulnerability, 219
 - activity, monitoring, 249–250
 - auctions, vulnerability, 218–219
 - kiosks, vulnerability, 223–224
 - limiting postings, 234–236
 - usage, vulnerability, 117–118. *See also* crime, on the Internet
- intrusion detection/prevention, 280–281
- inventory tracking, vulnerability, 132
- investments, vulnerability, 220–221
- Iran, threats posed by, 98–99
- Iranian hostage crisis, 10
- Iraq, presidential visit to, 109
- Ira's Four Golden Rules, 235
- IRM (information resource management), 47
- Israel, threats posed by, 93–94
- Ivanov, Alexey
 - administrator skills, 210
 - alert failure, 210
 - Amazon.com fraud, 203–204
 - background, 202–204
 - case summary, 208–209
 - casinovega.com break-in, 205–207
 - credit card fraud, 206–207
 - culture relations, 212–213
 - eBay fraud, 203–204
 - extortion, 206–207
 - front organizations, 204–205
 - getting caught, 207
 - international relations, 212–213
 - Lightrealm attack, 205–206
 - making of, 201–202
 - password exposures, 213
 - PayPal fraud, 204
 - perceived expense of security, 211–212
 - phishing schemes, 204–205
 - programming errors, 209–210
 - restitution, 209
 - security awareness, 212
 - security consultant skills, 211
 - undetected compromises, 210
 - unnecessary data, 212
 - vulnerabilities exploited, 209
 - web-hosting break-ins, 205–207

- Jacobs, Irwin, 100
- Japan, threats posed by, 95–97
- labeling computers, 159, 176, 179
- laptop theft, 100, 215
- laws, SB 1386 (duty to report penetration), 44
- layoffs, cellular telephone networks, 198
- legal filings, as information source, 25
- Levin, Vladimir, 216
- library control, 272
- lightning, 55
- Lightrealm attack, 205–206
- listening devices, 151, 290–291
- locks
 - cable, 271
 - card access, 275
 - on dumpsters, 273
 - espionage simulation, nuclear power plant, 172, 178
 - on information, 268–269
 - insufficient, 134
 - perimeter, 274
 - vulnerability, 134
- logs
 - audit, 289–290
 - clearing, 236–237
 - mirrored, 290
- low morale, cellular telephone networks, 198
- “Make money fast” schemes, 223–224
- malevolence *versus* malignancy, 65–66
- malicious software, 225–226
- malignancy *versus* malevolence, 65–66
- malware, 59–60
 - See also* bugs (software errors)
 - See also* program vulnerabilities
 - See also* technical countermeasures
 - See also* viruses and worms
- management buy-in and support, 298–301
- management weakness, vulnerability, 137–138
- managing risk. *See also* assessing risk; threat categories
 - assessment process, 33–34
 - balancing point, 36–38
 - balancing vulnerabilities and countermeasures, 36–38
 - budgeting for, 38–39
 - chemical and biological attacks, 32
 - cost/risk relationship, 36–38
 - gas masks, 32
 - mathematical model. *See* risk equation
 - maximizing countermeasures, 35
 - optimizing risk, 35
 - overreacting to risk, 31–32
 - plastic sheets and duct tape, 32
 - sample scenarios, 38–39
 - security programs, 34–35
 - spy’s view, 34
 - underreacting to risk, 31
- Marion, Pierre, 16
- marketing, vulnerability, 115–116
- meetings, as information source, 27
- mental weaknesses of agents, 8–9
- messy desks, vulnerability, 132
- MICE (Money, Ideology, Coercion, Ego), 8–9, 137
- Military Structure section, 83
- Minihan, Ken, 52
- mirrored logs, 290
- miscellaneous records, as information source, 25–26
- misrouted transactions, 72
- modem access, vulnerability, 146–147
- modem highjacking, 221
- monetary value of assets, 42–43
- money, as motivation, 8
- Money, Ideology, Coercion, Ego (MICE), 8–9, 137
- monitors, spying on, 149–150
- morale, 198, 239
- motivation of agents, 8–9
- motor vehicles, failure to check, 185, 188
- multifactor authentication, 287–288
- multilevel marketing, 222–223
- NASA Mars probe, costs of damage, 54
- national intelligence collectors, threats posed by, 67–68
- neighbors, vulnerability, 130
- Nimda worm, 141
- NOC (non-official cover), 7

- Nolan, John, 52, 62
- nondisclosure/noncompete agreements, 246–247
- non-official cover (NOC), 7
- nuclear power plant, espionage simulation
 - acquiring badges, 172–173
 - badge verification, 172–173, 178
 - blueprints exposed, 175, 179
 - case summary, 177
 - computer auditing, 176–177, 179
 - computer security, 175, 179
 - ID verification, 172, 177–178
 - labeling computers, 176, 179
 - locks, 172, 178
 - security guards, 173
 - social engineering, 172–176
 - tailgating, 173
 - unauthorized penetration, 173–177
 - universal badges, 178
 - vulnerabilities exploited, 177–179
- nuisance value, 46–48

- observation areas, airports, 188
- office pirates, 131–132
- off-line data storage, 292
- offshoring, threats posed by, 65
- off-site business, espionage countermeasures, 277
- O'Neill, Paul, 63
- on-site nonemployees, threats posed by, 64–65
- Open Source Intelligence (OSINT), 15
- open storage, vulnerability, 128–129
- operational countermeasures
 - awareness training, 238–241
 - badges, 246
 - call backs, 243–244
 - caller ID, verifying, 243–244
 - cellular phone conversations, limiting, 254
 - classifying information, 241–242
 - competitors, 248–249
 - conversations outside work, limiting, 254
 - cordless phone conversations, limiting, 254
 - disaster recovery, 256–257
 - employee morale, 239
 - giving advice, 239
 - guidelines for marketers and salespeople, 248
 - hacker training, 252
 - hackers as consultants, 258–259
 - ID, verifying, 244–245
 - incident handling, 256–257
 - information access, verifying need for, 244–245
 - Infraguard, 252–253
 - interdepartmental security, 255–256
 - Internet activity, monitoring, 249–250
 - minimizing data storage, 250
 - nondisclosure/noncompete agreements, 246–247
 - overview, 238
 - penetration testing, 259–260
 - phone conversations, limiting, 253–254
 - predictability, 255
 - Professional organizations, 252–253
 - reviewing corporate releases, 247–248
 - rewards, 243
 - security alert systems, 242–243
 - separate phone lines, 253
 - technical training, 251
 - technical vulnerabilities, monitoring, 250–251
 - vulnerability assessments, 257, 259–260
- operational vulnerabilities
 - accidents, 113
 - accounting for, 108–109
 - carelessness, 113
 - common sense and knowledge, 110–111
 - contractual relationships, 125
 - conversations, 119–120
 - credit cards, 119
 - help wanted ads, 117
 - human weakness, 123–124
 - Internet usage, 117–118
 - marketing, 115–116
 - overview, 108–109
 - personal aggrandizement, 121–122
 - policies and procedures, 113–114
 - poor awareness, 109–113
 - poor reporting procedures, 123

- operational vulnerabilities (*Continued*)
 - predictability, 114
 - procedures in practice, 115
 - public relations, 116–117
 - reverse social engineering, 112–113
 - sales, 115–116
 - social engineering, 111–112
 - supplier records, 120–121
 - telephone records, 119–120
 - too little information, 124
 - travel records, 119
 - working outside the office, 122–123
- operatives. *See also* agents; collectors
 - black bag operations, 10–11
 - definition, 6
 - NOC (non-official cover), 7
 - recruiting, 7
 - training, 7
- optimizing risk. *See* risk management
- organized crime, 71–74, 82
- OSINT (Open Source Intelligence), 15
- outsourcing, threats posed by, 65
- overreacting to risk, 31–32

- Painter, Christopher, 52
- passwords
 - exposures, 133–134, 144–145, 213
 - phishing for, 219
 - screen savers, 269
 - Windows 95 vulnerability, 141
- PayPal fraud, 204
- penetration testing, espionage counter-
measures, 259–260
- perceived information value, 41
- perfect crime, 4
- perimeter locks, 274
- perimeter security, espionage simulation,
157–158, 160, 166
- personal aggrandizement, 121–122
- personal hardship, 139–140
- personnel countermeasures. *See also*
employees; insiders
 - background checks, 261
 - employee hotlines, 262
 - employee roles, establishing, 265–266
 - employees, categorizing, 265–266
 - HR, coordinating with IS, 262–263
 - HR, coordinating with security
department, 263–264
 - information access, tracking, 264
 - overview, 260–261
 - requirements on contracted services,
267–268
 - security professionals, checking, 267
 - spouse checks, 262
 - terminations, coordinating, 266–267
 - visitors, reviewing, 264–265
- personnel vulnerabilities
 - background checks, 136–137
 - isolation of human resources, 138–139
 - MICE (Money, Ideology, Coercion,
Ego), 137
 - overview, 136
 - personal hardship, 139–140
 - separation procedures, 138
 - weak management, 137–138
- petty crime, threats posed by, 100–101
- phishers
 - costs of damage, 59
 - description, 224–225
 - Internet schemes, 204–205
 - for passwords, 219
- phreakers, threats posed by, 75
- physical assets, value, 42–43
- physical controls, airports, 183, 186
- physical countermeasures
 - badges, 274–275
 - cable locks, 271
 - card access locks, 275
 - choosing a location, 276
 - clean desk policies, 270
 - copy machine controls, 271–272
 - dumpster locks, 273
 - facility walk-throughs, 270
 - fire suppression, 277
 - guard training, 275–276
 - information locks, 268–269
 - library control, 272
 - off-site business, 277
 - overview, 268
 - password protection, 269
 - perimeter locks, 274
 - recycle bins, 273
 - removal of equipment, 274

- screen savers, 269
- security patrols, 276
- security reminders, 272
- shredders, 272–273
- strange postings, 270–271
- unusual access, 274
- UPSs (uninterruptible power supplies), 277–278
- physical vulnerabilities
 - access controls, 127
 - computers not logged out, 133
 - copy machines, 129
 - electrical systems, 134–135
 - electronic storage, 129
 - environment, 130–131
 - equipment size, 131–132
 - garbage, 127–128
 - inboxes, 132–133
 - insufficient locks, 134
 - inventory tracking, 132
 - messy desks, 132
 - neighbors, 130
 - office pirates, 131–132
 - open storage, 128–129
 - overview, 125
 - password exposures, 133–134
 - placement of buildings and equipment, 135
 - security guards, 126–127
- pizza delivery, social engineering scenario, 5
- plastic sheets and duct tape, risk management, 32
- policies and procedures, vulnerability, 113–114
- Political section, 83
- pornography, 221
- power outages, 55, 277–278
- predictability, 114, 255
- presidential visit to Iraq, 109
- the press, as information source, 26
- preventive measures
 - See case studies
 - See countermeasures
 - See security programs
 - See threat categories
 - See vulnerabilities
- prime rule of espionage, 3
- procedures in practice, vulnerability, 115
- Professional organizations, 252–253
- program vulnerabilities. *See also* technical countermeasures; technical vulnerabilities; viruses and worms
 - buffer overflows, 141
 - costs of damage, 54
 - malware, 59–60
 - software bugs, 140–143
 - Windows 95 passwords, 141
- program vulnerabilities, viruses and worms
 - Blaster, 141
 - Code Red, 141
 - costs of damage, 58–59
 - Nimda, 141
 - Slammer, 141
- programming errors, Internet vulnerability, 209–210
- public relations, vulnerability, 116–117
- pyramid schemes, 222–223
- recruiting agents
 - China, 86, 87
 - disgruntled employees, 62
 - espionage simulation, 162
 - France, 90
 - Israel, 93–94
 - mental weaknesses, 8–10
 - MICE (Money, Ideology, Coercion, Ego), 8–10
 - motivation, 8–10
 - typical case, 7
- recycle bins, espionage countermeasures, 273
- regulatory filings, as information source, 25
- reporting procedures, 123, 169
- requirements definition phase, 12–14
- restitution, 209
- reverse social engineering, 112–113. *See also* social engineering
- rewards, espionage countermeasures, 243
- risk equation
 - countermeasures factor, 33
 - overview, 32–33
 - threat factor, 33
 - value factor, 32
 - vulnerability factor, 33

- risk management. *See also* threat categories
 - assessment process, 33–34
 - balancing point, 36–38
 - balancing vulnerabilities and countermeasures, 36–38
 - budgeting for, 38–39
 - chemical and biological attacks, 32
 - cost/risk relationship, 36–38
 - gas masks, 32
 - mathematical model. *See* risk equation
 - maximizing countermeasures, 35
 - optimizing risk, 35
 - overreacting to risk, 31–32
 - plastic sheets and duct tape, 32
 - sample scenarios, 38–39
 - security programs, 34–35
 - spy's view, 34
 - underreacting to risk, 31
- Russia, threats posed by, 81–85
- Russian intelligence document, 83–84

- safe cars, 35
- sales, vulnerability, 115–116
- SB 1386 (duty to report penetration), 44
- Schweizer, Peter, 91
- scrap paper, as information source, 24
- screen savers, 269
- script kiddies, threats posed by, 78–80
- security alert systems, 242–243
- security awareness
 - crimes against individuals, 227
 - espionage simulation, 169
 - programs, 302
 - vulnerability, 212
- security consultants
 - checking, 267
 - hackers as, 258–259
 - skill levels, 211
 - threats posed by, 64–65
- security guards
 - airports, 184, 187
 - failure to challenge strangers, 161, 173
 - failure to investigate suspicious activity, 163
 - perimeter security, 157
 - training, 166–167, 275–276
 - vulnerability, 126–127
- security patrols, 276
- security professionals. *See* consultants
- security programs, developing
 - corporate culture, 298
 - countermeasures, choosing, 296–298
 - crying wolf, 303
 - description, 34–35
 - determining value, 295
 - and homeland security, 302–304
 - listing vulnerabilities, 295
 - management buy-in and support, 298–301
- security reminders, 272
- sensitive information exposed, 188
- separation procedures
 - coordinating terminations, 266–267
 - severance assistance, 198
 - vulnerabilities, 138
- separation procedures, vulnerability, 138
- severance
 - assistance packages, 198
 - coordinating terminations, 266–267
 - separation procedures, 138
 - vulnerabilities, 138
- severance assistance, cellular telephone networks, 198
- Sheymov, Victor, 52
- shredders, 272–273
- SIGINT (Signals Intelligence), 15
- Signals Intelligence (SIGINT), 15
- single sign-on software, 288
- Slammer worm, 141
- social engineering. *See also* reverse social engineering
 - espionage simulation (Fortune 500 company), 160–161
 - espionage simulation (nuclear power plant), 172–176
 - pizza delivery, 5
 - pretext phone calls, 111
 - vulnerability, 111–112
- social security numbers as IDs, 160, 169
- software
 - See also* malware
 - See also* program vulnerabilities
 - See also* technical vulnerabilities
 - See also* viruses and worms
 - testing, 286

- software, bugs
 - Gorshkov, Vasily, 209–210
 - Ivanov, Alexey, 209–210
 - programming errors, 209–210
 - technical vulnerabilities, 140–143
 - Wall Street programming errors, 54
- software errors (bugs)
 - Gorshkov, Vasily, 209–210
 - Ivanov, Alexey, 209–210
 - programming errors, 209–210
 - technical vulnerabilities, 140–143
 - Wall Street programming errors, 54
- spam, costs of damage, 58
- spammers, 58
- special agents, 5–6
- spies
 - See also* agents
 - See also* collectors
 - See also* criminals
 - See also* hackers
 - See also* operatives
 - See also* phishers
 - See also* phreakers
 - See also* spies
 - Bond, James, 3
 - Bristow, Sidney, 3, 305
 - common perception, 4
 - risk management, 34
- spouse checks, 262
- spying. *See* espionage
- spying on monitors, 149–150
- spyware, 59–60, 148–149, 225–226
- standard analysis, 18
- stock tips, vulnerability, 220–221
- Studeman, William, 72
- Sullivan, Bob, 217
- supplier records, vulnerability, 120–121
- suppliers, threats posed by, 101–102
- surveillance, detecting, 163–164
- system modifications, vulnerability, 148
- system utilities, as countermeasures, 237
- tailgating
 - airports, 183, 186
 - Fortune 500 company, 158, 170
 - nuclear power plant, 173
 - tampering with evaluation results, 19
- technical countermeasures. *See also* program vulnerabilities
 - anti-virus software, 279
 - audit logs, 289–290
 - automated patching, 285–286
 - backups, 281–283
 - bug sweeps, 290–291
 - business continuity, 282
 - configuration baselines, 286–287
 - disaster recovery, 282
 - encryption, 291–292
 - firewalls, 279–280
 - intrusion detection/prevention, 280–281
 - mirrored logs, 290
 - multifactor authentication, 287–288
 - off-line data storage, 292
 - overview, 278
 - single sign-on software, 288
 - software testing, 286
 - vulnerability scanners, 283
 - war dialing, 283–284
 - wireless security, 284–285
 - wiretap sweeps, 290–291
- technical training, 251
- technical vulnerabilities
 - bugs (listening devices), 151
 - bugs (software error), 140–143
 - configuration errors, 143–144
 - data transmission, 147–148
 - EMPs (electromagnetic pulses), 150
 - firewalls, 146–147
 - modem access, 146–147
 - monitoring, 250–251
 - overview, 140
 - password exposures, 144–145
 - spying on monitors, 149–150
 - spyware, 148–149
 - system modifications, 148
 - telephone taps, 150–151
 - TEMPEST, 149–150
 - Van Eck radiation, 149–150
 - war dialing, 147
 - wardriving, 146–147
 - warmarking, 146
 - wireless networks, 145–146

- telecommunications access, espionage
 - simulation (Fortune 500 company), 168–169
- telephone conversations, limiting, 253–254
- telephone records, vulnerability, 119–120
- telephone taps, 150–151
- telephones, separate lines, 253
- TEMPEST, 149–150
- temporary files, clearing, 236–237
- temporary workers, threats posed by, 64–65
- terminations, coordinating, 266–267
- terrorists, threats posed by, 68–71
- third-party intelligence collectors, threats posed by, 67–68
- threat categories. *See also* risk
 - accidents, 53–54
 - acts of God, 54–56
 - competitors, 103–105
 - crackers, 75
 - customers, 102
 - earthquakes, 55
 - fires, 55
 - floods, 55
 - hackers, 74–75, 78–80
 - human errors, 53–54
 - hurricanes, 55
 - information warriors, 66–67
 - lightning, 55
 - malignancy *versus* malevolence, 65–66
 - national intelligence collectors, 67–68
 - organized crime, 71–74
 - petty crime, 100–101
 - phreakers, 75
 - power outages, 55
 - script kiddies, 78–80
 - suppliers, 101–102
 - terrorists, 68–71
 - third-party intelligence collectors, 67–68
- threat categories, common criminals
 - credit card fraudsters, 57–58
 - identity thieves, 56–57
 - malware, 59–60
 - phishers, 59
 - spammers, 58
 - spyware, 59–60
 - viruses, 58–59
 - worms, 58–59
- threat categories, countries
 - China, 85–90
 - Cuba, 99–100
 - France, 90–92
 - Germany, 94–95
 - India, 97–98
 - Iran, 98–99
 - Israel, 93–94
 - Japan, 95–97
 - overview, 80–81
 - Russia, 81–85
- threat categories, insiders
 - consultants, 64–65
 - departing workers, 63
 - disgruntled employees, 62–63
 - employees, 60–62
 - former employees, 63–64
 - offshoring, 65
 - on-site nonemployees, 64–65
 - outsourcing, 65
 - temporary workers, 64–65
 - thrill seekers, 63
- threat factor, risk equations, 33
- threats posed by, lightning, 55
- thrill seekers, threats posed by, 63
- Toys “Я” Us, information value, 45
- traffic analysis, 18
- training operatives, 7
- TRASHINT, 15
- travel records, vulnerability, 119
- travel scams, 220
- underreacting to risk, 31
- undetected compromises, vulnerability, 210
- uninterruptible power supplies (UPSs), 277–278
- unlimited document access, 199
- unnecessary data, vulnerability, 212
- UPSs (uninterruptible power supplies), 277–278
- vacation scams, 220
- value factor, risk equations, 32
- Van Eck radiation, 149–150
- verifying IDs
 - callers, 243–244
 - in person, 172, 177–178, 244–245

- Verton, Dan, 71
- viruses and worms
 - Blaster, 141
 - Code Red, 141
 - Nimda, 141
 - Slammer, 141
- visitors, reviewing, 264–265
- vulnerabilities. *See also* case studies;
espionage simulation
 - balancing with countermeasures, 36–38
 - defensive measures *See* countermeasures
 - finding, 140–143
- vulnerabilities, airport simulation
 - attack, 183–185
 - failure to check IDs, 184, 187–188
 - failure to motor vehicles, 185, 188
 - inconsistent security, 184, 187
 - observation areas, 188
 - physical controls, 183, 186
 - security guards, 184, 187
 - sensitive information exposed, 188
 - tailgating, 183, 186
 - watching the obvious, 184, 186
- vulnerabilities, cellular telephone networks
 - auditing, 199
 - CD capacity, 199
 - centralized document storage, 199
 - layoffs, 198
 - low morale, 198
 - severance assistance, 198
 - unlimited document access, 199
- vulnerabilities, exploited
 - airports, 186–188
 - cellular telephone networks, 196–199
 - crime, against individuals, 226–227
 - crime, on the Internet, 209
 - nuclear power plant, 177–179
- vulnerabilities, Fortune 500 company
 - simulation
 - computer access, 159, 168
 - construction procedures, 159, 167
 - labeling computers, 159
 - lack of escorts, 167–168
 - no challenge to strangers, 157, 161, 169–170
 - perimeter security, 157–158, 160, 166
 - reporting procedures, 169
 - security awareness, 169
 - security guards, 157, 161, 163, 166–167
 - social engineering, 160–161
 - social security numbers as IDs, 160, 169
 - tailgating, 158, 170
 - telecommunications access, 168–169
- vulnerabilities, nuclear power plant
 - simulation
 - acquiring badges, 172–173
 - badge verification, 172–173, 178
 - blueprints exposed, 175, 179
 - computer auditing, 176–177, 179
 - computer security, 175, 179
 - ID verification, 172, 177–178
 - labeling computers, 176, 179
 - locks, 172, 178
 - security guards, 173
 - social engineering, 172–176
 - tailgating, 173
 - unauthorized penetration, 173–177
 - universal badges, 178
- vulnerabilities, operational
 - accidents, 113
 - accounting for, 108–109
 - carelessness, 113
 - common sense and knowledge, 110–111
 - contractual relationships, 125
 - conversations, 119–120
 - credit cards, 119
 - help wanted ads, 117
 - human weakness, 123–124
 - Internet usage, 117–118
 - marketing, 115–116
 - overview, 108–109
 - personal aggrandizement, 121–122
 - policies and procedures, 113–114
 - poor awareness, 109–113
 - poor reporting procedures, 123
 - predictability, 114
 - procedures in practice, 115
 - public relations, 116–117
 - reverse social engineering, 112–113
 - sales, 115–116
 - social engineering, 111–112
 - supplier records, 120–121

- vulnerabilities, operational (*Continued*)
 - telephone records, 119–120
 - too little information, 124
 - travel records, 119
 - working outside the office, 122–123
- vulnerabilities, personnel
 - background checks, 136–137
 - isolation of human resources, 138–139
 - MICE (Money, Ideology, Coercion, Ego), 137
 - overview, 136
 - personal hardship, 139–140
 - separation procedures, 138
 - weak management, 137–138
- vulnerabilities, physical
 - access controls, 127
 - computers not logged out, 133
 - copy machines, 129
 - electrical systems, 134–135
 - electronic storage, 129
 - environment, 130–131
 - equipment size, 131–132
 - garbage, 127–128
 - inboxes, 132–133
 - insufficient locks, 134
 - inventory tracking, 132
 - messy desks, 132
 - neighbors, 130
 - office pirates, 131–132
 - open storage, 128–129
 - overview, 125
 - password exposures, 133–134
 - placement of buildings and equipment, 135
 - security guards, 126–127
- vulnerabilities, technical. *See also* program vulnerabilities; viruses and worms
 - bugs (listening devices), 151
 - bugs (software error), 140–143
 - configuration errors, 143–144
 - data transmission, 147–148
 - EMPs (electromagnetic pulses), 150
 - firewalls, 146–147
 - modem access, 146–147
 - monitoring, 250–251
 - overview, 140
 - password exposures, 144–145
 - spying on monitors, 149–150
 - spyware, 148–149
 - system modifications, 148
 - telephone taps, 150–151
 - TEMPEST, 149–150
 - Van Eck radiation, 149–150
 - war dialing, 147
 - wardriving, 146–147
 - warmarking, 146
 - wireless networks, 145–146
- vulnerability assessments, 257, 259–260
- vulnerability factor, risk equations, 33
- vulnerability scanners, 283

- war dialing, 147, 283–284
- wardriving, 146–147
- warmarking, 146
- watching the obvious, 184, 186
- web cramming, 220
- web-hosting break-ins, 205–207
- Windows 95 passwords, 141
- wireless networks, vulnerability, 145–146
- wireless security, 284–285
- wiretap sweeps, 290–291
- Woolsey, James, 52
- Worcester Airport hack, 147
- work-at-home schemes, 223–224
- working outside the office, 122–123
- working papers, as information source, 24
- worms. *See* viruses and worms

- zombie networks, 60, 73
- zombie software, 226

