

Index

• A •

- access cards, 168
 - access control
 - archive protection, 257–258
 - comprehensive remediation, 245–248
 - implementing, 54
 - IT security, 116
 - NAC, 243–245
 - overview, 239–240
 - protection of classified content, 237
 - role-based, 273
 - self-auditing, 63
 - tightening, 240–243
 - acquisition, data, 207
 - acquisitions and mergers (M&A), 44, 94, 171, 236, 328
 - add-ons, browser, 262
 - address bar, 384
 - Administrative standard, HIPAA, 51
 - administrator access, 130, 340
 - administrator password, 192, 284
 - administrator privileges, 159
 - advertising, 357
 - adware, 111, 386
 - agentless technology, 143
 - agents
 - defined, 143
 - mail-transfer, 200
 - NAC, 247–248
 - self-enforcement, 242
 - “allow” and “deny” functionality, 159
 - anomaly detection, IDS, 225–226
 - answering machines, 287
 - anti-adware software, 386
 - anti-malware software, 129, 157, 159, 176, 385
 - anti-phishing filter, 135, 385
 - anti-spam software, 135, 183, 188
 - anti-spyware software, 188, 386
 - anti-threat technology, evolution of, 114–117
 - anti-virus software
 - archive protection, 257
 - effectiveness of, 180, 224
 - endpoint security, 134
 - overview, 115
 - spear phishing, 188
 - updating, 129, 157, 159, 176, 385
 - appliances, inline encryption, 255
 - applications
 - analyzing access, 361–362
 - data corruption, 267–270
 - data integrity
 - Open Source software, 272–273
 - overview, 271
 - periodic review of, 274–275
 - testing, 273
 - identification of, 63
 - malicious code targeted at, 18
 - management of, 219
 - monitoring, 41
 - SaaS, 275–277
 - Web
 - Internet browsers, 261–265
 - overview, 259
 - SQL injection attacks, 260–261
- archiving data
 - data classification, 208
 - identifying risk, 256–257
 - overview, 331
 - protecting corporate memory, 257–258
- ARP poisoning, 243
- asset management, 157, 219
- Atom Flash Drive, 140–141
- at-risk data
 - bank data, 92
 - corporate data, 33, 94–95
 - credit cards, 92

at-risk data (*continued*)

- customer communication, 93–94
 - customer data, 32–33, 95
 - customer-loyalty cards, 92–93
 - data at rest, 31
 - data in motion, 31–32
 - e-mail, 93–94
 - finding
 - derivatives, 35
 - matching data to locations, 35–37
 - obvious locations, 34–35
 - overview, 33
 - health and welfare information, 94
 - overview, 91
 - zippering, 96
- auction account information, 100–101
- audit logs, 270, 365
- audits
- automating, 64–65
 - backup tape, 253
 - benefits of, 62–63
 - compliance technology requirements, 62
 - fees, 68
 - for governance, 332–333
 - information-security, 338–339
 - overview, 61–63
 - regularity of, 41
 - self-audits, 62–64
 - tools for, 135
- authorization control
- comprehensive remediation, 245–248
 - NAC, 243–245
 - overview, 239–240
 - tightening, 240–243
- automatic address-search function, 204
- automatic code checkers, 271
- automatic data-loss prevention system, 212
- automatic form-filler application, 129
- automatic system control, 184
- automating audits, 64–65
- Availability, CIA model, 88
- availability risks, IT, 21
- awareness program
- culture, 324
 - ongoing, 323
 - security training, 322–323

• **B** •

- backdooring, 130, 163, 272–273
- background checks, contractor, 309–310
- backup
 - disk-based, 254
 - hardware encryption, 254–256
 - overview, 251–252
 - process for, 320
 - protection of, 231
 - SIS, 331
 - tape-based
 - destroying, 281
 - encryption, 255
 - environment, 253
 - overview, 32, 251–253
- bandwidth, 356
- bank data, 92, 100, 105
- banking
 - dangers of online, 121
 - passwords, 384
 - regulation, 52–53
- Basel II Accord, 52–53
- BC (business continuity), 321
- behavioral analysis, 261, 362–364
- BIOS password, 150
- black market, 37–38, 112
- blackmail, 38
- blind trust, 380
- blocked e-mail, 202
- blocking USB devices, 135, 144
- blogs, 16, 95
- bluebugging, 163
- bluejacking, 163
- bluesnarfing, 163
- Bluetooth
 - overview, 161
 - solutions for, 162
 - turning off, 193
 - vulnerabilities, 162–163, 289
- boot order, 150
- boot-image control, 228
- botnet, 111–112
- bots, 111, 130, 231
- brand damage, 69, 79, 103

briefing sessions, press, 354
bulk sale of information, 102
business continuity (BC), 321
business operation procedures, 358
business record, 11
business social-networking sites, 369–370

• C •

cached certificates, 126
caching, 233
calendars, 155
cameras, 288
Canadian regulation, 55
Capability Maturity Model Integration (CMMI), 318–319
cardholder data protection, 54
Cardtrp threat, 155
CD-ROMs
 destroying, 281
 encrypting data to and sending, 303
 free, 141, 170–171, 174
 overview, 32
cellular phones. *See* mobile phones
central management, 229
centralized backup, 230
CEO (Chief Executive Officer), 353
certificates, 126
Chief Information Officer (CIO), 24, 326, 353
Chief Information Risk Officer (CIRO), 24, 326, 353
Chief Information Security Officer (CISO), 24, 326, 353
CIA model, 87–88
CIO (Chief Information Officer), 24, 326, 353
CIRO (Chief Information Risk Officer), 24, 326, 353
CISO (Chief Information Security Officer), 24, 326, 353
cleaners, 130, 310
cleaning data, 147
clickjacking, 264
CMMI (Capability Maturity Model Integration), 318–319
COBIT (Control Objectives for Information and related Technology), 317
code, software, 268
code checkers, automatic, 271
code reviews, 261, 274–275
company information, 33, 94–95
compensation, customer, 68
competitors, 99
compliance
 audits
 automating, 64–65
 compliance technology requirements, 62
 overview, 61–63
 self-audits, 63–64
 DLM/ILM as aid to, 208–209
 documenting, 169
 full disclosure, 48–49
 good governance, 58–61
 risks, 21
compression, 255
conferences, 170–171, 288, 293
Confidential classification level, 366
confidential data, 74, 142–143
Confidentiality, CIA model, 87
connectivity, 156, 159
consent, data subject, 57
consistency, 329
consultants, 130, 339
contact details, posting, 369
content filtering, 116, 135
content management, 223
content-aware discovery technology, 160
content-based encryption policies, 145–146, 236
content-classification software, 91
content-matching technology, 236–237
context, data, 29, 31
Continual service improvement, ITIL, 315
contractors, 130, 309–310
contracts, 57
Control Compliance Suite, 332
Control Objectives for Information and related Technology (COBIT), 317
cookies, 265
copying data, 35, 237

- corporate data, 33, 94–95
 - corporate firewall, 226
 - corporate network connections
 - choosing, 134
 - thin-client technology, 132
 - virtualizing clients, 133
 - VPNs, 131–132
 - costs
 - of downtime, 89
 - of response, 68
 - counterfeit credit cards, 75
 - covert monitoring, 41
 - CRCs (Cyclic Redundancy Checks), 269
 - credit-card data, 92, 100, 105
 - credit checks, 103
 - credit monitoring, 68
 - critical system protection (CSP), 227
 - crosscut shredder, 294
 - cross-site scripting, 262–264
 - CSP (critical system protection), 227
 - customer access, 339
 - customer churn, 69
 - customer communication, 93–94
 - customer compensation, 68
 - customer data, 32–33, 95, 103, 160
 - customer lists, 105
 - customer notification, 351
 - customer support, 355–356, 357
 - customer-loyalty cards, 92–93
 - customer-support call centers, 47
 - cut-and-paste, 129
 - cyber-café, 169, 172–173
 - cyber-crime
 - clickjacking, 264
 - controlling, 76–77
 - data corruption, 364–365
 - DDoS attacks, 231
 - dumpster diving, 309
 - e-mail scams, 93
 - flooding, 232
 - law enforcement, 76
 - overview, 17–19, 71–75
 - piggybacking, 308–309
 - session poisoning, 265
 - smurf attacks, 232
 - social-engineering attacks, 308
 - spear phishing, 187–188
 - SQL injection attacks, 260–261
 - targeting corporate information, 42
 - use of data, 37–38
 - XSS attacks, 262–264
 - zippering, 96
 - cyber-criminals
 - evolution of, 112–113
 - mentality of, 113
 - monetary value of data to
 - availability of data, 101–102
 - finding data on Web, 102–104
 - over lifetime, 104–105
 - overview, 99
 - popular data, 100–101
 - overview, 10–11
 - priorities of, 117
 - Cyclic Redundancy Checks (CRCs), 269
- D •
- damage limitation, 350
 - data acquisition, 207
 - data at rest
 - NAC, 244–245
 - overview, 31
 - data breaches
 - regulations for, 50
 - sources of, 73–74
 - data center
 - data availability, 224–225
 - DoS attacks, 231–234
 - encryption
 - content-based, 236
 - difficulty of, 235–236
 - managing digital rights, 237–238
 - overview, 234
 - outsiders in, 339
 - overview, 217–218
 - protecting server infrastructure
 - centralized backup, 230
 - CSP, 227

- endpoints, 228–230
- overview, 226–227
- servers, 228–230
- thin-client technology, 228–230
- unstructured data files, 218–221
- data classification
 - consistent, 211–212
 - DLM/ILM, 206–210
 - good governance, 59
 - overview, 205–206
- data corruption
 - guarding against, 268–269
 - malicious, 364–365
 - overview, 267–268
 - performance, 269–270
- data deduplication, 222
- data feed checks, 269
- data in motion
 - NAC, 244
 - overview, 31–32
 - protecting, 377
- data integrity
 - Open Source software, 272–273
 - overview, 271
 - periodic review of, 274–275
 - testing, 273
- data loss. *See also* at-risk data; cyber-crime
 - comprehensive approach to
 - counteracting
 - evaluating risk, 78
 - overview, 77–78
 - prospect of fines, 80
 - protecting IT, 81–82
 - risk of jail time, 80–81
 - understanding damage to reputation, 79
 - factors involved in
 - cyber-crime, 17–19
 - e-commerce, 12–14
 - gadgets, loss of, 10–11
 - ignorance, 19–20, 381
 - information management, 15
 - messaging boom, 11–12
 - storage capacity, 14–15
 - Web 2.0, 16–17
 - full disclosure, 71–72
 - hardware disposal
 - destroying electronic data, 281–283
 - overview, 279–280
 - system repair, 283–284
 - without losing data, 283
 - holistic perspective of, 25–27
 - identifying data sources
 - answering machines, 287
 - conference calls, 288
 - digital cameras, 288
 - e-mail archives, 284–285
 - facsimiles, 286
 - miscellaneous, 289–290
 - photocopiers, 286–287
 - printers, 286–287
 - remote access, 288–289
 - SMS, 285
 - VoIP, 287
 - Webcasts, 288
 - overview, 9–10, 349–350
 - people who cause, 37–42
 - rethinking data security
 - considering options, 85
 - monetary value of data, 83–85
 - overview, 82–83
 - responsibility, 85–86
 - risks and consequences of
 - direct losses, 67–68
 - electronic records, 23–24
 - indirect losses, 68–69
 - IT risk, 20–23
 - total cost, 70–71
 - secrecy about, 379
 - steps to take in event of
 - media, 353–354
 - mobilization, 352–353
 - ongoing project, 354–358
 - plan creation, 350–352
 - treating as disaster, 321–322
- Data Protection Act 1998 — U.K., 43
- Data Protection Directive 1995 — E.U., 43–44
- data retention, 206–207, 210, 223

- data security
 - considering options for, 85
 - data classification
 - consistent, 211–212
 - DLM/ILM, 206–210
 - overview, 205–206
 - e-mail
 - endpoint security, 183–186
 - evolving threats from, 182–183
 - overview, 181–182
 - hardware appliances, 193–194
 - messaging systems
 - instant messaging, 202–203
 - overview, 197–199
 - protecting e-mail, 199–200
 - Web-based e-mail, 200–202
 - the wrong Dave, 203–205
 - monetary value of data, 83–85
 - overview, 82–83, 179–181, 195–196
 - policies for, 59, 83, 138
 - protecting intellectual property, 196
 - recognizing potential security holes, 212–215
 - responsibility, 85–86
 - spear phishing, 187–189
 - wireless security, 190–193
- data segregation, 344
- databases
 - bank-account details, 92
 - credit-card data, 92
 - encryption of, 235
 - extracts, 270
 - restricting access to fields in, 365
 - storage of data on, 34
- data-breach notification laws, 58
- data-discovery technology, 143–144
- data-feed checking, 273
- data-flow diagramming, 296–297
- data/information lifecycle management (DLM/ILM), 206–210
- data-loss crisis team
 - creating, 326–327
 - tasks for, 327
- data-loss prevention (DLP), 25–26, 60, 144–145, 196
- data-matching technology, 236
- data-protection laws, 43–44
- data-source checking, 273
- date of birth, posting, 369
- DDoS (distributed DoS) attack, 231
- Defined level, CMM, 318
- deleting data, 147, 213, 331–332
- denial-of-service attack. *See* DoS attack
- Deskstar drive, 140
- desktop virtualization, 228
- destroying electronic data, 281–283
- destructive viruses, 111
- device-control technology, 116
- devices. *See also* laptops; mobile phones; PDAs; USB devices
 - loss of, 10–11
 - management of, 219
 - risk factors, 90–91
- DHCP (Dynamic Host-Configuration Protocol), 193
- DHCP Enforcer, 242–243
- digital cameras, 288
- digital rights, managing, 237–238
- direct losses, 67–68
- Directive on the Protection of Personal Data, E.U., 58
- disaster recovery (DR), 157, 321
- discover phase, NAC, 245–246
- discovery
 - monitoring and enforcement policies, 144–145
 - moving on from, 329–330
 - overview, 59, 327–328
 - technology for, 143–144, 160
- disk-based backup, 254
- disposal of hardware
 - destroying electronic data, 281–283
 - overview, 279–280
 - policy for, 300
 - revisiting, 377
 - system repair, 283–284
 - without losing data, 283

dissolvable agents, 247
distributed DoS (DDoS) attack, 231
distribution lists, 300
DLM/ILM (data/information lifecycle management), 206–210
DLP (data-loss prevention), 25–26, 60, 144–145, 196
DNS (Domain Name System), 232–234
document disposal, 300
document-matching technology, 236–237
Domain Name System (DNS), 232–234
DoS attack (denial-of-service attack)
 flooding, 232
 overview, 231–232
 poisoned DNS, 232–234
downtime, cost of, 89
DR (disaster recovery), 157, 321
drive-by pharming, 191
drops, 101
dumb terminals, 132
dumpster diving, 309
DuPont company, 360
DVDs, 32, 281. *See also* CD-ROMs
Dynamic Host-Configuration Protocol (DHCP), 193
dynamic IP addresses, 193

• E •

eavesdropping, 312
e-commerce, 12–14
Economist Intelligence Unit, 155
e-crime. *See* cyber-crime
eDRM (enterprise digital rights management), 125–126, 135, 238
education
 about CD-ROM use, 312
 about cyber-café, 174
 about evil twin threat, 172
 about paper disposal, 291
 about phishing, 188
 about USB device use, 312
 about XSS attacks, 264
 of employees, 370–371, 379
 for new hires, 175

education-and-awareness program, 377–378
electronic access card, 168
Electronic Protected Health Information (EPHI), 51
electronic records, 23–24
e-mail
 addresses, 93, 101
 archives, 284–285
 automatic address-search function, 204
 communication via, 93–94
 content-classification software on cellular phones, 91
 data in motion, 31
 database lists, 112
 endpoint security, 183–186
 evolving threats from, 182–183
 importance of, 11
 overview, 181–182
 passwords, 101
 protecting, 199–200
 sensitive data in, 24–25, 171, 300
 storage of data in, 34
 Web-based, 31, 35, 200–202
embedded encryption, 255
employees
 behavior policies, 95, 97
 education of, 370–371, 379
 malicious, 40–41
 notifying
 of data loss, 353
 of threats, 114
 sensitivity of data about, 94
encryption keys, 126, 255
encryption strategies
 for backup tapes, 252
 cardholder data protection, 54
 for CDs, 303
 choosing, 127–128
 for data center
 content-based, 236
 difficulty of, 235–236
 managing digital rights, 237–238
 overview, 234

- encryption strategies (*continued*)
 - for data on disks, 270
 - for database extracts, 270
 - eDRM, 125–126
 - file-based encryption, 125
 - full-disk encryption, 124–125
 - for hardware, 254–256
 - hiding data with, 365
 - for Hitachi Deskstar drive, 140
 - for laptops, 150–151
 - for mobile devices, 158–159
 - for offsite data, 376
 - overview, 123–124
 - on Web sites, 265
 - for Wi-Fi equipment, 192
 - endpoint evaluation technologies, NAC, 243
 - endpoint security
 - consolidating, 152
 - control of functionality, 159
 - e-mail, 183–186
 - encryption technologies
 - choosing, 127–128
 - eDRM, 125–126
 - file-based encryption, 125
 - full-disk encryption, 124–125
 - overview, 123–124
 - keyloggers, 128–129
 - laptops, 121–123
 - network connections, 131–134
 - overview, 75
 - protecting
 - priority, 376
 - products for, 134–136
 - server infrastructure, 228–230
 - risks to, 119–122
 - rootkits, 130–131
 - virtualization, 167
 - enforce phase, NAC, 245–246
 - enforcers, NAC, 243
 - enhancement requests, 342
 - enterprise digital rights management (eDRM), 125–126, 135, 238
 - EPAL (Enterprise Privacy Authorization Language), 61
 - EPHI (Electronic Protected Health Information), 51
 - ePrivacy Directive, 50
 - escape characters, 261
 - ET software, 151
 - E.U. Directive on the Protection of Personal Data, 58
 - European Convention on Human Rights, 56
 - European regulations, 56
 - European Union regulations
 - common restrictions on processing data, 57
 - implications of, 57–58
 - overview, 56
 - “evil twin” threat, 172
 - exhibitions, 170–171
 - Extensible Access Control Markup Language (XACML), 61
- F ●**
- facsimiles, 286
 - family education, 385
 - FAQs (Frequently Asked Questions), 356
 - faxes, 286
 - Federal Trade Commission, U. S., 85
 - file protection, Windows, 365–366
 - File Transfer Protocol (FTP), 201
 - file-based encryption, 125, 135
 - filtering
 - anti-phishing, 135, 385
 - content, 116, 135
 - USB device, 135
 - financial data, 92, 94, 100, 103–105
 - financial privacy, 45, 52
 - Financial Privacy Rule, 52
 - financial statements, 104
 - finest, 67–68
 - firewall
 - attention to, 192
 - compared to IDS, 226
 - endpoint protection, 135
 - hardware, 176

- keylogger prevention, 129
- overview, 115
- protection by, 179–180
- FireWire, 289
- firmware, 159
- flip chart, 292
- flooding, 232
- fluffing, 281
- Formula 1 teams, 360
- fraud, 38, 352
- free credit monitoring, 47
- freebies, 170–171, 174, 311–312
- Frequently Asked Questions (FAQs), 356
- FTP (File Transfer Protocol), 201
- full disclosure
 - compliance with, 48–49
 - cyber-crime and, 71–72
 - overview, 46–48, 50
 - regulations, 51–55
- full-disk encryption, 124–125, 128, 135
- functionality checking, 269, 273

• G •

- geography
 - location-based access control
 - changing policies, 166–167
 - merging logical and physical security, 167–169
 - overview, 165–166
 - risks
 - conferences, 170–171
 - exhibitions, 170–171
 - free USB devices, 170–171, 174
 - holiday and vacation infections, 173–174
 - Internet cafés, 172
 - mergers and acquisitions, 171
 - new hires, 175
 - overview, 169
 - working from home, 175–176
- governance
 - auditing for, 332–333
 - balancing privacy and data protection, 60–61

- data classification, 59
- data-loss prevention solutions, 60
- overview, 58
- record retention and retrieval, 59–60
- Governance Risk and Compliance (GRC)
 - policy, 332
- government classifications, 366–367
- Gramm-Leach-Bliley, 52
- GRC (Governance Risk and Compliance)
 - policy, 332

• H •

- hacker targets, 74
- hard drives, 281, 286–287
- hardware encryption
 - compression, 255
 - encryption keys, 255
 - overview, 254–255
 - SaaS, 256
- hardware firewall, 176
- hardware improvements, 210
- hardware-recovery software, 151
- health and welfare information, 94, 104
- Health Insurance Portability and Accountability Act (HIPAA), 51
- Her Majesty's Revenue and Customs (HMRC), 47–48
- hiding data
 - information sensitivity and access, 366–367
 - overview, 365–366
 - real-time redaction, 367–368
- HIPAA (Health Insurance Portability and Accountability Act), 51
- Hitachi Deskstar drive, 140
- HMRC (Her Majesty's Revenue and Customs), 47–48
- holiday infections, 173–174
- holidays, posting, 369
- holistic perspective
 - knowledge and control, 25
 - mind map, 26–27
 - wide approach, 25–26

home network, locking down, 384
 Homeland Security Presidential Directive (HSPD-12), 169
 host-based IDS, 226
 HTTP (Hypertext Transfer Protocol), 201
 human-resource data, 94

• 1 •

icons, used in book, 5–6
 identification
 equipment, 168
 individual, 168, 310
 identities, sale of, 100
 IDS (intrusion-detection system), 116, 135, 225
 IDS anomaly detection, 225–226
 IDS misuse detection, 225
 ignorance, 19–20, 379
 ILM (information lifecycle management), 219–220
 IM (Instant Messenger), 32, 182
 Imation Atom Flash Drive, 140–141
 impersonation, 310–311
 implicit trust
 analyzing application access, 361–362
 analyzing user behavior, 362–364
 malicious data corruption, 364–365
 overview, 359–361, 379, 381
 inactive data, 208
 incentive programs, 324
 incineration, 282
 indirect losses, 68–69
 information lifecycle management (ILM), 219–220
 information management, 15
 Information Rights Management (IRM), 366
 information risk management, 218
 information technology. *See* IT
 information-protection policy
 auditing for governance, 332–333
 consistency, 329, 381
 data-loss crisis team, 326–327
 discovery, 327–330
 new hires, 175
 overview, 41, 325–326
 reducing data, 331–332
 of third parties, 343
 information-security policy, 55, 85–86, 338–339. *See also* data security
 informing customers. *See* full disclosure
 Initial level, CMM, 318
 in-line blocking, 243
 inline encryption appliances, 255
 in-line NAC, 243
 insecure business process, 314
 insider trading, 104
 insiders, malicious, 126
 instant messaging, 19, 202–203, 285
 Instant Messenger (IM), 32, 182
 Integrity, CIA model, 87
 intellectual property, 94, 105, 125, 160, 196
 internal leakage, 81–82
 International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27002, 317–318
 international regulations
 Canada, 55
 Europe, 56
 European Union, 56–58
 United States, 56
 international trading, 65
 Internet bandwidth, 356
 Internet browsers
 address bar, 384
 clickjacking, 264
 cross-site scripting, 262–264
 overview, 261–262
 plug-ins, 262, 386
 session hijacking, 265
 Internet cafés, 169, 172–173
 Internet privacy, 45
 Internet Relay Chat (IRC), 102
 Internet Security Threat Report, 156
 Internet-based communication, 32, 35, 182, 202–203. *See also* e-mail
 interview techniques, 298–299

intrusion-detection system (IDS), 116, 135, 225
 intrusion-prevention system (IPS), 116, 135, 226
 investigation fees, 68
 iPod, 32
 IPS (intrusion-prevention system), 116, 135, 226
 IRC (Internet Relay Chat), 102
 IRM (Information Rights Management), 366
 ISO/IEC (International Organization for Standardization/International Electrotechnical Commission) 27002, 317–318
 IT (information technology)
 management of, 210, 219
 security
 basics of, 114–117
 risks, 20–23
 threat landscape, 109–112
 IT department, 327, 350, 358
 ITIL (IT Infrastructure Library), 314–316

● **K** ●

keylogger software, 121, 310

● **L** ●

LAN 802.1X Enforcer, 243
 laptops
 company policy for, 174
 customer data on, 320
 “evil twin” threat, 172
 locking down, 149–152
 loss of, 10, 41–42, 89, 122–123, 170
 overview, 121–122
 personal data on, 383–384
 protecting, 123
 solutions for, 134
 traveling with, 122
 wireless networks, 191
 law enforcement, 76

laws. *See* regulations
 lawsuits, 49, 68
 legal department, 122, 350
 legal hold, 332
 legal obligations, 57
 legislation. *See* regulations
 lifecycle-management policy, 186
 LinkedIn, 370
 litigation, 68
 live data storage, 331
 locking down
 home networks, 384
 laptops, 149–152
 wireless connection points, 176
 wireless routers, 191–193
 logical archive protection, 257
 logical audits, 41
 log-on, 168
 logos, corporate, 93
 long-term prevention
 information-protection policy
 auditing for governance, 332–333
 consistency, 329
 data-loss crisis team, 326–327
 discovery, 327–330
 overview, 325–326
 reducing data, 331–332
 revisiting decisions about, 333–335

● **M** ●

M&A (mergers and acquisitions), 44, 94, 171, 236, 328
 MAC addresses, 192
 macro viruses, 111
 magnets, 148–149, 282–283
 mail management tool, 151
 mailers, 101
 mail-security services, 188
 mail-transfer agent (MTA), 200
 malicious hacking, 17
 malicious insiders, 40–41, 99, 201, 260–261, 360–362
 malware, 113, 174, 263

- Managed level, CMM, 318
 - managerial security issues, 214–215
 - marketing campaigns, 47
 - marketing department, 122, 326, 351
 - massive repositories of structured data (MRSDs), 260
 - MDM (Mobile Device Management)
 - solutions, 158
 - media, dealing with
 - choosing spokesperson, 353–354
 - facts, 354
 - frequent updates, 354
 - medical privacy, 45
 - mergers and acquisitions (M&A), 44, 94, 171, 236, 328
 - messaging boom, 11–12
 - messaging systems. *See also* e-mail
 - instant messaging, 202–203
 - overview, 197–199
 - the wrong Dave, 203–205
 - Microsoft Outlook, 204
 - mind map, 26–27
 - minnowing, 189
 - mirroring, 140–141
 - misuse detection, IDS, 225
 - mitigating actions, 47
 - Mobile Device Management (MDM)
 - solutions, 158
 - mobile phones
 - Bluetooth, 161–163
 - cameras on, 288
 - controlling functionality on, 158–161
 - e-mail on, 91
 - loss of, 10, 90–91
 - overview, 153–154
 - protecting, 155–158, 163–164
 - risks and benefits of, 154
 - SMS, 285
 - mobile-device security policies, 154
 - modems, 289–290
 - monetary value of data
 - to criminals
 - availability of data, 101–102
 - finding data on Web, 102–104
 - over lifetime, 104–105
 - overview, 99
 - popular data, 100–101
 - by customer, 84
 - by employee time, 84–85
 - hourly rate, 84
 - identifying at-risk data
 - bank data, 92
 - corporate data, 94–95
 - credit cards, 92
 - customer communication, 93–94
 - customer data, 95
 - customer-loyalty cards, 92–93
 - e-mail addresses, 93
 - e-mail communication, 93–94
 - health and welfare information, 94
 - overview, 91
 - zippering, 96
 - modeling information
 - devices, 90–91
 - markets, 91
 - overview, 87–89
 - risk and consequences, 89
 - overview, 83–84
 - total cost, 97–98
 - monitor phase, NAC, 245–246
 - monitoring
 - data, 105
 - NAC, 243
 - networks, 54–55
 - MORI omnibus survey, 49
 - MRSDs (massive repositories of structured data), 260
 - MTA (mail-transfer agent), 200
 - multiple-user technologies, 16
 - My Book, 141
 - MySpace, 11
- *N* ●
- NAC (network access control)
 - agents, 247–248
 - control aspect, 219
 - data at rest, 244–245

- data in motion, 244
- endpoint security, 135
- overview, 116, 239–241, 243–244
- PCI DSS standard, 54
- nearline storage, 221
- negligent data loss, 39–40
- network access control. *See* NAC
- network connections
 - choosing, 134
 - printers, 287
 - thin-client technology, 132
 - virtualizing clients, 133
 - VPNs, 131–132
- network intrusion detection, 180
- network management, 219
- network roaming capabilities, 159
- new hires, 175
- NIDS (network-based IDS), 226
- notepads, 155
- notification, customer, 351–352. *See also*
 - full disclosure
- notification letters, 47, 71

● 0 ●

- offsite backup storage, 252
- offsite shredding, 293
- offsite system repair, 283
- on-screen keyboards, 129
- onsite shredding, 293
- onsite system repair, 283
- Open Source software, 272–273
- Optimized level, CMM, 318
- Outlook application, 204
- overt system auditing, 41
- overwriting data, 281

● p ●

- P3P (Platform for Privacy Preferences), 61
- packet-sniffing programs, 201
- paired Bluetooth devices, 162
- parallel ports, 289

- parameterized statements, 261
- parity, 140
- partners
 - preventing loss by
 - data center, 339
 - information-security audits, 338–339
 - overview, 337–338
 - SaaS providers, 339–340
 - service oriented architectures, 341
 - trust in, 342–345
- passive IDS, 226, 245
- passwords
 - changing for administrator, 192
 - eavesdropping for, 312
 - encryption, 123–125, 235
 - Internet banking, 384
 - mobile devices, 154
 - overview, 48–49
 - protection of, 213
 - strength of, 150
 - during system repair, 284
 - thin-client systems, 132
 - usernames, 50
- patch management, 156–157, 180
- pattern-based data, 237
- Pbstealer threat, 155
- PCI DSS (Payment Card Industry Data Security Standard), 53–55, 65, 270, 319
- PDAs
 - Bluetooth, 161–163
 - controlling functionality on, 158–161
 - overview, 153–154
 - protecting, 155–158, 163–164
 - risks and benefits of, 154
- peer-to-peer enforcement, 242
- penetration testing, 188, 311
- performance, storage, 210
- performance risks, IT, 21
- perimeter firewall, 180
- perimeter security, 186
- persistent agents, 247
- personal activities, 45
- personal data, 55–58, 213
- personal firewall, 115, 135, 180

- personal identifiable information (PII), 11, 44
 - Personal Information Protection and Electronic Documents Act (PIPEDA), 55
 - pharming, 175–176, 191
 - phishing
 - applications, 112
 - context of information, 30
 - information used for, 369
 - overview, 18, 111, 182–183
 - warning customers of, 103
 - phone lines, 355
 - phonebooks, 155
 - photocopiers, 126–127, 286–287
 - physical addresses, 192
 - physical audits, 41
 - physical laptop-security policy, 121–122
 - Physical standard, HIPAA, 51
 - pictures, work site, 95, 97, 368–369
 - piggybacking, 308–309
 - PII (personal identifiable information), 11, 44
 - PINs, mobile device, 154
 - PIPEDA (Personal Information Protection and Electronic Documents Act), 55
 - piracy, 103
 - Platform for Privacy Preferences (P3P), 61
 - Plaxo, 370
 - Plug and Play gateway appliances, 194
 - plug-ins, browser, 262
 - points of failure, 229
 - poisoned DNS, 232–234
 - policies
 - content-based encryption, 145–146, 236
 - data security, 59, 83, 138
 - developing, 301
 - discovery monitoring and enforcement, 144–145
 - e-mail, 201–202
 - employee behavior, 95, 97
 - encryption-key, 126
 - IM, 202–203
 - information protection, 175
 - informing users about, 186
 - mobile device, 121–122, 154, 174
 - NAC, 243
 - people factor
 - interview techniques, 298–299
 - overview, 295–296
 - work groups, 296–298
 - refining, 330
 - security, 85–86
 - shredding, 293
 - storage-security, 148–149
 - that put data at risk, 300–304
 - policy engine, 205
 - policy-based appliances, 61
 - political affiliations, 45
 - Ponemon Institute, 70–71, 74, 290
 - pop-up blocker, 385
 - PR (public relations), 326, 351
 - pretexting, 52, 311
 - Pretexting Protection rule, 52
 - pricing information, 94, 105
 - printed data
 - cleaning up after meetings, 292–293
 - overview, 290–291
 - revisiting destruction of, 377
 - shredding policy, 293–294, 383
 - warning signs, 291–292
 - printers, 286–287
 - privacy, 45, 51–52, 60–61
 - Privacy Rule, HIPAA, 51
 - proactive threat management, 138
 - product-design documents, 94
 - project office, 352
 - proof of care, 77
 - protection management, 223
 - proxies, 101
 - public relations (PR), 326, 351
 - purging, 147
 - push technology, 144
- *Q* •
- quarantine, laptop, 151
 - questions, interview, 298–299

• R •

- RAID (Redundant Array of Independent Disks), 140–141
- reactive IDS, 226
- real-time redaction, 367–368
- record retention and retrieval, 59–60
- recruiting, cyber-crime, 38
- redaction technology, 365
- reducing data
 - archiving, 331
 - deleting, 331–332
 - to single instance, 331
- Redundant Array of Independent Disks (RAID), 140–141
- re-evaluating procedures, 320–321
- regulated industry, 65
- regulations
 - audits, 46–48
 - changes in, 333
 - DLM, 208–209
 - full disclosure
 - Basel II Accord, 52–53
 - compliance with, 48–49
 - cyber-crime and, 71–72
 - Gramm-Leach-Bliley, 52
 - HIPAA, 51
 - overview, 46–48, 50
 - PCI DSS, 53–55
 - international
 - Canada, 55
 - Europe, 56
 - European Union, 56–58
 - United States, 56
 - overview, 43–46
 - passwords, 48
 - relevancy, 65
- religious bias, 44
- remedial action, 68
- remediate phase, NAC, 245–246
- remediation workflow, 164
- remote access, 288–289
- remote administration, 193
- remote wipe and kill, 160–161
- removable media
 - careless use of, 141–142
 - destroying data on, 146–149
 - evolution of, 139–141
 - identifying, 376
 - locking down laptops, 149–152
 - overview, 137–139
 - strategies for dealing with
 - content-based encryption policies, 145–146
 - discovery monitoring and enforcement policies, 144–145
 - overview, 142–144
 - USB ports, 144
- repair personnel, 130
- repairing hardware, 283–284
- Repeatable level, CMM, 318
- reporting restrictions, 270
- reports
 - data loss, 76
 - database, 35
 - incidence, 151
- reputation damage, 69, 101
- research and development, malware, 113
- Restricted classification level, 367
- restricted data, 23
- restricted partitions, 365
- retention management, 223
- retention policy, 331–332
- right-to-know principle, 47
- ring-fence access, 167, 228
- risk. *See* at-risk data; data loss; geography
- risk-assessment tool, 25
- road apples, 311
- road warriors, 122, 131, 134, 165
- root access, 130, 284

• S •

- SaaS (Software as a Service)
 - identifying threats, 276
 - overview, 275

- SaaS (Software as a Service) (*continued*)
 - preventing loss by third-party providers, 339–340
 - securing data from tampering, 276–277
- SaaS (Storage as a Service), 256
- Safe Harbor program, 56
- Safeguards Rule, 52
- sales
 - bad publicity, 327
 - loss of, 68
 - malware, 113
 - promotions, 357
- SB 1386 (U.S. security-breach disclosure law), 72
- scanning, wireless network, 190–191
- scans, laptop, 151
- screen scrapers, 75
- scripting, 264
- secondary checks, 265
- Secret classification level, 366
- secure networks, 54
- Secure Socket Layer (SSL) certificate, 234
- Secure Socket Layer (SSL) encryption, 265
- securing individual computers, 213
- security, data. *See* data security
- security code reviews, 274–275
- security management, 219, 223
- security policies, 85–86, 186
- security reviews, 23
- security risks, IT, 21
- Security Standards Rule, HIPAA, 51
- security-breach disclosure law (SB 1386), U.S., 72
- self-audits, 62–64
- selling data, 38
- sensitive data
 - identifying, 375–376, 380
 - M&A process, 171
 - overview, 366–367
 - policies that risk, 300
 - types of, 44–45
- serial ports, 289
- server infrastructure
 - centralized backup, 230
 - CSP, 227
 - endpoints, 228–230
 - overview, 226–227
 - thin-client computing, 228–230
- server management, 219
- Service design, ITIL, 315
- Service Level Agreement (SLA), 343
- Service operation, ITIL, 315
- service oriented architectures, 341
- service providers, 343–345
- Service strategy, ITIL, 315
- Service transition, ITIL, 315
- services, sharing, 16
- session hijacking, 265
- session key, 265
- settlements, 67–68
- sexual orientation, 44
- share price, 69
- Short Message Service (SMS), 19, 202–203, 285
- shredding
 - cleaning up after meetings, 292–293
 - hard disks, 281
 - overview, 147, 290–291
 - personal information, 383
 - policy for, 293
 - revisiting, 377
 - shredders, 294
 - warning signs, 291–292
- signing in, 384
- SIS (Single Instance Storage), 331
- skip diving, 309
- SLA (Service Level Agreement), 343
- sleep mode, 128
- smishing, 19
- SMS (Short Message Service), 19, 202–203, 285
- smurf attacks, 232
- social networking
 - data loss, 371–372
 - overview, 368–370
 - phishing, 370
- social-engineering attacks
 - contractors, 309–310
 - defined, 18–19, 30, 120
 - dumpster diving, 309

- eavesdropping, 312
 - freebies, 311–312
 - impersonation, 310–311
 - piggybacking, 308–309
 - software
 - archive protection, 257
 - distribution of, 156–158
 - updating, 129, 157, 159, 176, 323, 385
 - Software as a Service. *See* SaaS
 - Software Security Engineering Capability Maturity Model (SSE-CMM), 318–319
 - source code, 94
 - spam, 18, 42, 109, 182–183
 - spear phishing
 - minnowing, 189
 - overview, 187
 - shields against, 188
 - traffic shaping, 188
 - whaling, 189
 - speech recognition, 129
 - spim, 182
 - spokesperson, 353–354
 - spreadsheets, 35–36
 - spyware, 111, 151
 - SQL injection attacks
 - overview, 260–261
 - preventing, 261
 - SRM (Storage Resource Management), 25
 - SSE-CMM (Software Security Engineering Capability Maturity Model), 318–319
 - SSID, 192
 - SSL (Secure Socket Layer) certificate, 234
 - SSL (Secure Socket Layer) encryption, 265
 - standards
 - choosing, 319
 - CMMI, 318–319
 - COBIT, 317
 - ISO/IEC 27002, 317–318
 - ITIL, 314–316
 - need for, 313–314
 - PCI DSS, 319
 - SSE-CMM, 318–319
 - storage
 - capacity, 14–15
 - management of, 219, 222–223
 - performance of, 210
 - security policies, 148–149
 - of sensitive information, 237
 - Storage as a Service (SaaS), 256
 - Storage Resource Management (SRM), 25
 - strip shredder, 294
 - striping, 140
 - structured data, 217
 - suppliers
 - preventing loss by
 - data center, 339
 - information-security audits, 338–339
 - overview, 337–338
 - SaaS providers, 339–340
 - service oriented architectures, 341
 - trust in, 342–345
 - support, malware, 113
 - support desks, 355–356
 - surveillance, 168
 - suspend mode, 128
 - Symantec Control Compliance Suite, 332
 - Symantec Internet Security Threat Report, 156
 - Symantec MORI omnibus survey, 49
 - Symantec Vontu Data Loss Prevention software, 329
 - synchronization, 131
 - system auditing, 41
 - system scans, 151
 - systemic data loss, 39
- **T** ●
- tailgating, 308–309
 - tape-based backup
 - destroying, 281
 - encryption, 255
 - environment, 253
 - overview, 32, 251–253
 - TB (terabyte), 139
 - TCO (total cost of ownership), 210
 - team building, 350–351
 - Technical standard, HIPAA, 51
 - technology changes, 334–335
 - telephone lines, 355

- telephones. *See* mobile phones
 - templates, 61
 - terabyte (TB), 139
 - test scams, 188
 - tests, security system, 54–55
 - text phishing, 19
 - thin-client technology, 132, 152, 228–230
 - third-party
 - data loss, 337–338
 - functionality checking, 273
 - trust in, 342–345
 - threat changes, 334
 - threat landscape
 - evolution of cyber-criminals, 112–113
 - mentality of cyber-criminals, 113
 - overview, 109–112
 - throttling, 183, 188
 - Time to Live property, 233
 - to-do lists, 155
 - Top Secret classification level, 366
 - total cost of ownership (TCO), 210
 - tracking
 - equipment, 168
 - individuals, 167
 - trading, international, 65
 - traffic shaping, 183, 188
 - transaction details, 105
 - transient encryption, 255
 - types, 261
- U •
- U. S. Federal Trade Commission, 85
 - Unclassified classification level, 367
 - underground economy, 18, 37–38, 100–101, 112
 - United Kingdom
 - cost per record lost in, 70–71
 - criminalization of data loss, 80
 - Driving Standards Agency records, 256
 - HMRC data, 47–48, 256
 - MORI omnibus survey, 49
 - United States, regulations, 56
 - Universal Declaration of Human Rights, Article 12, 45
 - unstructured data files
 - content defines value, 220–221
 - minimizing number of copies, 221
 - overview, 34–35, 218–219
 - updating
 - anti-malware software, 159, 385
 - anti-virus software, 129, 157, 159, 176, 385
 - security-awareness program, 323
 - uptime for data, 210
 - U.S. security-breach disclosure law (SB 1386), 72
 - USB devices
 - careless use of, 141–142
 - criminal use of, 128
 - destroying data on, 146–149
 - evolution of, 139–141
 - filtering and blocking of, 135
 - free, 170–171, 174, 311–312
 - locking down laptops, 149–152
 - overview, 137–139
 - strategies for dealing with
 - content-based encryption policies, 145–146
 - discovery monitoring and enforcement policies, 144–145
 - overview, 142–144
 - USB ports, 144
 - use of, 32
 - viruses on, 170–171, 174
 - USB ports, 144
 - Use Case, 296–297
 - user behavior, analyzing, 362–364
 - user error, 27
 - user privileges, 159
 - user-level security issues, 212
 - username, 50
- V •
- vacation infections, 173–174
 - vacations, posting, 369
 - virtual LANs, 243
 - virtual machines, 133
 - virtual private network (VPN), 131–132, 159, 172, 289–290

virtualization, 133, 167, 194, 228, 371–372
 viruses
 encryption and, 146
 example of, 120
 on free devices, 170–171
 scanning for on laptops, 151
 threat of, 109–112
 vishing, 19
 voice phishing, 19
 VoIP, 287
 Vontu Data Loss Prevention software, 329
 VPN (virtual private network), 131–132,
 159, 172, 289–290
 vulnerability scanner, 116
 vulnerability-management program, 54

• W •

wardriving, 175, 191
 Waste Electrical and Electronic Equipment
 (WEEE) Regulations, 280
 Web 2.0, 16–17, 371
 Web applications. *See also* applications
 Internet browsers
 clickjacking, 264
 cross-site scripting, 262–264
 overview, 261–262
 plug-ins, 262
 session hijacking, 265
 overview, 259
 SQL injection attacks, 260–261
 Web history, 156
 Web Service Privacy (WS-Privacy), 61
 Web services, 16
 Web-based e-mail, 31, 35, 200–202

Webcasts, 288
 Web-site checker, 385
 WEEE (Waste Electrical and Electronic
 Equipment) Regulations, 280
 Western Digital My Book, 141
 whaling, 189
 whiteboards, 292
 Wi-Fi locators, 191
 wikis, 16
 Windows file protection, 365–366
 wipe-and-kill functionality, 159
 wireless LAN (WLAN) transmitter, 191
 wireless networks, 151, 169–170, 175,
 191, 384
 wireless routers, locking down, 191–193
 wireless security
 drive-by pharming, 191
 locking down wireless routers, 191–193
 scanning for wireless networks, 190–191
 WLAN (wireless LAN) transmitter, 191
 work groups, 296–298
 working from home, 175–176
 worms, 111
 wrong Dave, the, 203–205
 WS-Privacy (Web Service Privacy), 61

• X •

XACML (Extensible Access Control Markup
 Language), 61

• Z •

zippering data, 96, 128

