Note: Page numbers in *italics* refer to Figures; those in **bold** to Tables.

acceptable use policy, 141–3, 169, 180, **197**, 246, 348, 351
conscious agreement, 141–2
improper nonofficial computer usage, 142
Michael A. Smyth v. The Pillsbury Company (case), 142–3
sample attributes, 141
team effort, 143
violations, 142
access control, 40, 42, 67, 72, 87, 121, 144, 166–70, 185, 244, 333, 348, 354
access control policy
discretionary, 185
mandatory, 185
role-base, 185
visitor and contractor agreement, 167
badging and identification, 167–8
check-outs, 168–9
designated parking, 166
electronics, 168
emergencies and evacuations, 168
enforcement, 169–70
network or system access, 169
reception, 166–7
tours, 169
American Civil Liberties Union (ACLU), 21
annualized loss expectancy (ALE), 58
annualized rate of occurrence (ARO), 58, 62–3
anonymous, 25, 26, 62, 68, 230, 309, 311, 312
anti-malware, 178
antispyware, 245
antivirus, 43, 104, 178, 180, 184, 186–7, 207, 245, 263, 283, 304, 305, 350, 354
AOL Time Warner, 126
auditing, 29, 47, 80, 89, 187, 198, 241, 267, 297, 307, 334, 350
authentication, 48, 162, 178, 194, 244, 352, 353
backdoor, 35, 43, 152, 254, 305, 353
Balanced Scorecard, 265–6
“Big Data,” 204–5
BigMIMS (medical information management system), 64, 67
BigRX
BigMIMS, 64, 67
business intelligence capability, 76
CEO, recommendations, 75–6
Corporation, 129–30
event likelihood, 67, 69–70
functional specifications, 132
incident impact, 70–71
new policy, 140
planning division, 130–132
Plieno Corporation, 64
risk assessments, 65
SQL injection vulnerability, 68, 129, 133, 135
testing procedures, 134
three-tier measurement techniques, 71
web pages, specifications, 132–3
BigRX plan, reduced SQL injection risk
additional resources, 137–8
applicability, 135
BigRX plan, reduced SQL injection risk (cont’d)
available resources, 137
execution, concept
contract modifications, 136
promotion to live system, 136–7
recurring performance management, 137
software procurement, contracts, 135–6
testing and acceptance, 136
governance
management reviews, 138–9
penetration testing, 138
vulnerability scanning, 138
purpose, 135
board involvement, levels, 336
boardroom interactions
cybersecurity audits, 334
cybersecurity risk management, corporate
culture, 331
goals and objectives, 329
hazard and operability study (HAZOP), 331
insurance, 334
levels of board involvement, 336
personnel vetting, 334
plan execution, 332
policy and procedures, 330
“Pollution Prevention Pays (3P)” program, 332
process control systems via intranet, 327
public relations and disaster recovery, 334
risk management, 326
strategy, 328
training, 334
botnet, 18, 19, 49, 302, 303

C2 see Command-and-control server (C2)
Canadian Cyber Incident Response Centre (CCIRC), 316
CEO or Chief Operating Officer, 189
Certified Associate in Software Testing (CAST) certification, 134
certified ethical hacker, 98, 195, 256, 306
Certified Information System Auditors (CISAs), 195
Certified Information Systems Manager (CISM), 234–6
Certified Information Systems Security Professional (CISSP), 234–6
Certified Manager of Software Testing (CMST), 134
Certified Software Tester certification (CSTE), 134
“CF Disclosure Guidance: Topic 2, Cybersecurity” (CF DG 2), 79
4chan, 25, 26
change management
backup plan, 220
best practices
asking for help, 221–2
backup and back-out plan, 223
communication, 220–221
crummy products, 221
flexibility, 224
maintenance, 222–3
monitor implementation, 223
software patches, 223–4
timing and needs, 221
best value, 203–4
catastrophe, 215
COA (courses of action) selection and management approval, 217–19
competitive advantage, 204–5
cyber attacks, 200
description, 199
downtime, 200
evaluation, 217
executives, 214, 215
fundamental responsibility, 214
identification, 217
impacts
capacity, 207–8
contracts, 206–7
people, 205–6
security, 208–9
SLAs, 206
and internal controls, 209–14
laws and regulations, 201
manufacturers, 216–17
monitoring and evaluation, 219
obsolescence, 201–3
organizational processes, 200
patch installation, 215
personnel, process and products, 200
risk environment, 200
steps, 215–16
technical measures, 214
chief financial officer (CFO), 58–9, 64, 129, 133, 135, 159, 209, 233, 241, 263, 307

chief information officer (CIO), 42

Chief Information Security Officer (CISO), 46, 47, 90, 132–9, 189, 218, 219, 233–7, 240, 241, 263

“career-broadening” jobs, 236

CISSP and CISM certifications, 234–5

credentials and experiences, 234
effectiveness, efficiency and security, 233–4

programs and operational activities, 233–4

software management and IT systems, 233

chief operating officer (COO), 58–9, 64, 133, 135, 137, 233

chief risk officer (CRO)

CISSP/CISM certifications, 236–7

corporate risk program, 90

risk appetite level, 91

Chief Security Officer (CSO), 196, 198, 233, 236, 237, 240

CIO see chief information officer (CIO)

CISM see Certified Information Systems Manager (CISM)

CISO see Chief Information Security Officer (CISO)

CISSP see Certified Information Security Professional (CISSP)

clean desk policy, 150–152, 197, 285, 349

best policy practices, 151–2

HIPAA, 150–151

Privacy Act, 151

cloud, 20, 42, 44–5, 45, 134, 138, 152, 181, 207, 264, 296, 348

command-and-control server (C2), 19, 26, 30, 48, 50

communication

exceptional, 113

internal see risk management

lack of, 113–14

shareholders see shareholders communications

Computer Ethics Policy

corporate ethics, 146–7

motivation, 146

Ten Commandments of Computer Ethics, 143–6

zero tolerance, 146

computer security

acceptable encryption, 347

acceptable use, 348

application service provider, 348

computer disaster recovery, 348

end-user encryption key protection, 348

password protection, 348

software installation, 348–9

workstation security, 349

confidentiality, 2, 214, 268, 294, 350

cookie, 154, 211

corporate espionage, 11

corporate ethics, 143, 146–7

cracker, 42

credentialing see employee credentialing

critical infrastructures

accident investigation, 252–3

ADS-B system, 251–2

audit, 258

automated control systems, 249–50

“bake in,” 256

business and industrial safety systems, 255

Chinese hackers, 254

computers and networks, 249

cyber attacks, 250

cybersecurity risks, 256–7

disruption, services, 253–4

enemies, 255

executives, 254–5

frightened workers, 252

hackers and terrorists, 249

ICS controls, 253

insurance policies, 250

monitor and control, 257

organizational priority, 256

personnel training, 257

power generation, turbine, 252

practice, 257–8

“pr0f,” 250–251

protection, 255

Sayano–Shushenskaya dam, 252

single points of failure, 257

“zero-defect” operations, 255

CRO see chief risk officer (CRO)

Cross-Site Scripting (XSS), 211–12

cryptography, 235

CSO see Chief Security Officer (CSO)

cyber Commandos, 343
cyber espionage, theft, and exploitation (checklist) see intellectual property and trade secrets

cybersecurity

as business imperative, 2–3

concerns

“bad actors,” 4
CEOs, 7
executive-level, 4
definition, 2

full-time activity, 7–8
generic questions, 4–6

incidents

by category, 281, 281

cost, 281–2
detection, 280–281

responsible for, 282, 282

incorporating into strategy

impacts in decisions, 119–20
information, identification, 119
as part of culture, 119, 331
progress, measuring, 120–121
risk management, 331
in management processes, 4
policies see policy(ies) complement plans
risk management, 3
strategy building, 95–7

Cybersecurity for Executives: A Practical Guide, 324
cyber threat sources, 12, 36, 55, 64, 68, 74, 78, 85

dashboards

acquisition, 285–6
change management, 284
competitions, 288–9

costs, 287
cybersecurity incidents, 281–2
employees, current cybersecurity training, 286

Executive Cybersecurity Dashboard, 289–90

industry experts, 289
industry groups and associations, 289

information loss/tampering/destruction, consequences, 287–8

network performance measures

current security software, devices, 283–4
previous measurements, 283, 283

physical security, 285
reporting period, security violations, 286
risk exposure, 288
security incidents/violations, 286
software configuration management, 284–5
system administrator privileges, 286
technical staff, current certifications, 286
threats detection

phishing messages, 278
quantitative measure, 278, 279
“repeat offenders,” charts, 277–8, 279
reverse lookup, 279

scans and probing, 277–8
spam filters, 278

value of information, 287
vulnerability see vulnerability(ies)

DDoS see distributed denial-of-service attack (DDoS)
defense-in-depth, 207, 257
degauss, 159
Delphi group technique, 70
demilitarized zones (DMZs), 244
denial-of-service attack, 19, 200, 278, 353
distributed denial-of-service attack (DDoS), 18, 26, 68, 200, 302, 312, 362

DMZ lab security, 353
Domain Name System (DNS), 159, 210
dynamic test environment, 134
electronic data interchange (EDI), 41, 213, 214, 353
electronic exchanges

businesses, 213
encryption, 213
system configurations, software and web pages, 212
third-party logistics providers (3PL), 213
United Airlines web page, 214

Electronic Mail Policy
account creation and removal, 175
directories and personas, 175
e-discovery, 173
etiquette rule, 173–4
internet-based resources, 172–3
mail forwarding, 174
mail retention, 175
email(s)

address, double checking, 357–8
attachments, 359
autoforward, 349
business and personal accounts, 359
caps lock key, 357
carbon copies, 358
emoticons, 359
junk/unwanted, 359
language, 357
professional font and color, 358–9
queries
apathy, 51–2
authentication, 48
curiosity, 52–3
digital signatures, 48
ignorance, 50
inadvertent disclosure, 49–50
Koobface versions, 49
lack of accountability, 54
lack of leadership, 53–4
negligence, 50–51
relevant and expected message, 48
social media, 48–9
stupidity, 52
retention, 349
signature blocks, 360
unnecessary replies, 360
usage, 349
employee credentialing
issuance, 170
tail-gating (drafting), 170
termination procedures, 171
usage, 170
Employee Internet Use Monitoring and Filtering Policy
applicability, 156
corporate policies, 155–6
enforcement, 158
filter rule, 157–8
monitoring, 156
purpose, 156
records, 156–7
reports, 156
encryption
acceptable, 347
electronic exchanges, 213
end-user, key protection, 348
equipment removal, 171–2
Estonia, 2007 cyber attack, 18–19
Executive Cybersecurity Dashboard, 289–90
Facebook software, misconfiguration, 210
facility controls
clutter, 165
double check, 165
locking information, 165
in and out checking, 165
rules, 165–6
surveillance and control, 165
temptation, 164–5
vigilant and trained, 165
Financial Services Modernization Act, 1999
see Gramm–Leach–Bliley Act (GLB)
Fortune, Robert, 9
freeware, 184
goals and objectives
affordable and suitable, 108
boardroom interactions, 329
business, aspects of, 110
definition, 108
organizational, 240, 265–6, 282
planning, 111, 121–2, 129, 190, 192, 197, 298
samples, 110
SMART goals, 108, 124
Gramm–Leach–Bliley Act (GLB), 194, 197, 263
hacking, managing
checklist, plan implementation
appropriate notifications, 307–9
damage, assessment, 305–7
defenses, adjustment, 310
external links, verification, 304–5
gaining control, 302–3
isolation, 302
panic, avoiding, 300–302
passwords, reset, 303–4
reason for hacking, 309–10
stealth drive, 305
update and scan, 304–5
computers types, 294
foot stompers
insurance, 317
law enforcement, working with, 315–17
legal discovery and associated requests, 319
hacking, managing (cont’d)

legal issues, 318–19
liability, addressing, 317–18
public relations (PR), importance, 310–315
trusted relationships, 318
2011 hack, of Sony Corporation’s PlayStation Network, example, 311–15
insurance, 317
Internet Crime Complaint Center (IC3), 316
personnels, watch on, 295
physical/network security measures, 293–5
plan implementation, 299–310
preparation see hacking, minimizing the impact
hacking, minimizing the impact
baseline documents, maintenance, 296–7
disaster recovery and business continuity plan, 298–9
information, back up, 296
insurance, protection, 297–8
natural disasters, 299
planning in advance, 299
regular audits, 296
hacktivists
Assange, 25
cyber threat sources, 12, 36
definition, 25
Low Orbit Ion Cannon, 26
Operation Payback, 26
WikiLeaks, 25–6
hashed, 148
hazard and operability study (HAZOP), 331
Health Insurance Portability and Accountability Act (HIPAA), 64
clean desk policy, 150–151
legal compliance concerns, 1996, 193–4
human risk management
email queries see email(s)
spear phishing and whaling, 48
hypertext markup language (HTML), 145
industrial control systems (ICS), 47
hacker, 250–251
manufacturing processes, 238–9
password, 251
smelting and casting process, 238
Stuxnet-like attack, 253
“industrial strength” disk wiping program, 160
information security, 350
Information Systems Auditing Standards, 195
insider threats
cyber threat sources, 12, 36
definition, 26–7
effect, 28
spear phishing, 28
insurance, 297–8, 317
Integrated Services Digital Network (ISDN) phone lines, 353
integrity, 2, 30, 41, 83, 118, 186, 194, 209, 212–14, 255, 271, 294
intellectual property and trade secrets
cyber espionage, theft, and exploitation (checklist)
competitors, 40
computer storage, 40
contracted system administration and software support, 42
data backups, 41
data feeds, 41
DVD/CD read-write drives, 41
intellectual property and trade secrets, 39
internet access, 40
off-site storage, 41
USB connections, 40
quantitative risk see quantitative risk assessment
internal controls
electronic exchanges, 212–14
organizations, 209
policies and procedures, 209
software, 210–211
system configurations, 209–10
web pages, 211–12
International Information Systems Security Consortium (ISC2), 234
International Standards Organization (ISO) 27001 (Information Security Management) certification, 264
Internet Crime Complaint Center (IC3), 316
Internet Protocol (IP) address, 157, 210, 279, 363, 364
Internet security
antivirus, 350
digital signature, 350–351
extranet, 351
monitoring and filtering, 351
remote access, 352
use, 351–2
Internet Use Policy
applicability, 153
employee’s actions, problems, 152
internet resources, misuse, 152–3
official business use, 153
prohibited Internet use, 153–4
purpose, 153
threats, 153
intranet, 202, 217, 238, 250, 270, 327, 351
IP address see Internet Protocol (IP) address
ISC2 see International Information Systems Security Consortium (ISC2)
ISC2’s ten domains, 235
Joint Universal Lessons Learned System (JULLS), 245
Keep It Simple, Stupid (K-I-S-S), 105
law enforcement, 315–17
legal compliance issues
Gramm–Leach–Bliley Act (GLB), 194
HIPAA of 1996, 193–4
Privacy Act of 1974, 194
Sarbanes–Oxley (SOX) Act of 2002, 193
legal discovery and associated requests, 319
legal issues, 318–19
liability, addressing, 317–18
Low Orbit Ion Cannon, 26
malware, 16, 48, 152, 187, 270, 301, 313, 354
management’s discussion and analysis (MD&A), 81–2
mechanics of strategy
core values, 107–8
deliberations
competencies, 106
effectiveness, 106
risk management, 106
value, 106
goals and objectives see goals and objectives
Keep It Simple, Stupid (K-I-S-S), 105
leadership, 98
mission statements, 107
resources, cyber-related, 103–4
simplicity, 105
SWOT see SWOT analysis
team effort, 98
trustworthy computing, 105
vision, 105–6
vision statement, 107
memory leak, 208
mercenary hackers
Hannibal Lecter of computer crime (Poulsen), 21
independent contractors, 20
Operation Firewall, 22
ShadowCrew, 22
SQL injection, 23
threats, 21
war driving, 23
messaging, 157, 186, 310
Metasploit, 200
metric categories, 277–88
metrics see also performance measures and C-suite
compliance, 274
cybersecurity questions, 275–7
cyber threats, 274
decision-making process, 275
executives, metrics decisions, 274–5
productivity and cybersecurity, 274
cybersecurity controls, 264
operational, 271–2
organizational, 271
performance measures, 262
selection, 265, 267
technical, 272
mission statements, 107
mobile device policy
acceptable use, 180
applications, 181
back-up and recovery, 181–2
business processes, 181
data plans, 180
devices, 179
information and risk, 179
legal considerations, 180
maintenance, 181
regulatory compliance, 179–80
security, 180–181
services, 180
mobile security, 352
modern IT, 128–9
multi-disciplinary “red teams,” 195–6

National Cyber Crime Unit (NCCU), UK, 316
National Cyber Security Alliance (NCSA), 51
National Industrial Security Program Operating Manual (NISPOM), 160

nation-state threats
China
Advance Persistent Threat 1, Mandiant’s report, 15
bad actors, 14
botnet ‘sleepers,’ 19
controversial activities, 16
cyber attacks, factors, 14
Cyber Corps, 13
Estimating the Cost of Cybercrime and Cyber Espionage, 17
Internet Security Report for 2013, Symantec Corporation, 16
cyber threat sources, 12, 36
DDoS attacks, 18
Estonia, 2007 cyber attack, 18–19
Russians, 19
natural disasters, 71, 299
Nessus, 200, 279
Netflix, 111–12
Netsploit, 14

network management policy
application security, 187
centralized logging, 188
deny all, permit by exception, 186
least privilege, 186
malware filtering, 187
“must-have” policy, 185–6
secure operating systems, 186
sensor architecture, 188
threat/incident analysis, 188
vulnerability management, 187

network security, 53, 72, 81, 294, 320, 353–4
Nmap, 200, 279

obsolescence
dumpster diver, 202
5.25 floppy disks and 3.5 diskettes, 201–2
hackers, 202–3
hardware and software, 202
typewriter and carbon paper, 201
web pages, 202
Windows XP computer, 202
Open Web Application Security Project, 129–30
Operation Edna, 116
Operation Firewall, 22
organized crime, 12, 20, 36

password(s) see also Password Protection Policy
best practices, 45–7, 148–9
creation and protection, 190, 206, 207, 244, 245, 348
cybersecurity risks, 45
default, 245, 251, 295
encryption and authentication, 355
forgetting, 35
one-time, 353
password-protected network, 169
practices, 45–6
regularly changed and complex, 21
remote access, 46–7
resetting, 35, 303–4, 321, 345
vulnerability scans, 46

Password Protection Policy
best practices, 148–9
“must-haves”
account lock-outs, 149
avoid transmitting passwords via email, 150
don’t recycle passwords, 150
force password expiration, 150
separate administrative and user passwords, 149
passphrases, 149
risk, 147–8
patching, 67, 71, 187, 202, 208–9, 212, 217–18
patch installation, 215
penetration test (Pen-test), 52, 66, 74, 101, 162, 170, 195, 219, 251, 258

performance measures
Balanced Scorecard concept, 265–6
business drivers
compliance, 270
cost, 267–8
quality, 269
return on investment, 269–70
risk, 268–9
safety, 270–271
cybersecurity metrics see metrics
decision-making, 265
due diligence and due care, 262–3
employees, reward and discipline, 266
executive cybersecurity dashboard see dashboards
information systems, 263
internal controls, 263
ISO 27001 certification, 264
nonpublic personal information, 263
partners and clients, agreements, 264
performance standards
accountability, 237
ICS, 238–9
malicious code, 238
measures, 238
monetary costs, 239
Pliendo Steel Company, 238
product, 239–40
wisdom and judgment, 237
zero tolerance program, 237
Personal Health Information (PHI), 194
personally identifiable information (PII), 130, 158, 160, 194
personnel management
business function and activity, 228
critical infrastructure protection, 249–58
leaders, 228–9
organizational considerations

corporate sponsor, 240

Financial Review Boards, 241
leadership, 240, 242
plans, policies and procedures, 241
risk committees, 241
performance standards, 237–40
plans, policies and procedures, 227
responsibilities, 227–8
system administration, 228
team creation, 229–37
threats and vulnerabilities, 228
training, 242–9
personnel vetting, 334
phishing, 244, 278, 281, 349
physical security policy
emergencies and evacuations, 172
employee credentialing, 170–171
equipment removal, 171–2
facility controls, 164–6
port security, 163
security checks, 163
visitor and contractor access controls, 166–70
PII see personally identifiable information (PII)
ping, 278, 279
plan execution, 332
plan implementation, 299–310
planning see also goals and objectives
acceptance and payment process, 133
in advance, 299
auditing, 195–6
BigRX Corporation, 129–30
characteristics, 127
coding issue, 133
dynamic test environment, 134
flexibility, 128
great teams, 131
Hurricane Katrina, aftermath, 192
internal controls, 133
legal compliance concerns, 193–4
modern IT, 128–9
operational level, 122, 130
organizations, level of perfection, 191–2
plan of action
business, protection, 129
cost-effective, 129
management of information, 128
policies and procedures, 129
vigilance and updates, 129
policies see policy(ies) complement plans
procedures see procedures implement plans
risk management systems, 129
SMART model, 132
SQL injection attacks, risk, 129–30
strategic level, 122, 130
tactical level, 122, 130
testing software, 133, 134
title, 131
Pliendo corporation
business intelligence capability, 76
revitalizing steel industry, 57, 213
risk management strategy, 73–6
policy(ies)
audit security, 347
boardroom interactions, 330
computer security, 347–9
desktop security, 349
policy(ies) (cont’d)
email, 349
information security, 350
Internet security, 350–352
mobile security, 352
network security, 353–4
physical security, 354
server security, 354
wireless devices, 354–5
policy(ies) complement plans
BigRX, new policy, 140
business rules and guidelines, 189–90
CEO or Chief Operating Officer, 189
corporate risk management processes, 188–9
cybersecurity
acceptable use policy, 141–3
access control policy, 185
clean desk policy, 150–152
computer ethics policy, 143–7
electronic mail policy, 172–5
employee internet use monitoring and filtering policy, 155–8
mobile device policy, 178–82
network management policy, 185–8
password protection policy, 147–50
physical security policy, 161–72
remote access policy, 177–8
removable media policy, 175–7
software policy, 182–5
technology disposal policy, 158–61
use of the internet policy, 152–5
Pollution Prevention Pays (3P) program, 332
port, 40, 162, 163, 175, 176, 186, 223, 304, 354
port scan, 14, 141
Privacy Act of 1974, 194
procedures implement plans
basic cyber hygiene, 191
cybersecurity plans and policies, 190
daily practice, 190–191
proxy, 40, 167, 187
Public Key Infrastructure (PKI), 45
public relations (PR)
disaster recovery, 334
importance, 310–315
quantitative risk assessment
BigMIMS, 66
BigRX, 67
Pen-testing, 66
scanning results, 66
system administrators, 66–7
Risk analysis, 57–8
Cyber incidents, 55
Intellectual property and trade secrets
acquisition or development, 56
assets value
loss, estimation
asset value (AV), 61
risk exposure (RE), 61
ceo, 57–8
Qualified risk assessment
BigMIMS, 64
HIPAA, 64
incident impact, definitions, 70–71
incident likelihood
Delphi group technique, 70
Microsoft products, 69
plurality rule! techniques, 70
measurement techniques, 71
risk and asset value, 63
risk decisions
acceptance, 72–3, 75, 76
avoidance, 73, 75, 76
BigRX CEO, 75–6
cybersecurity issues, 76–7
mitigation techniques, 71–2, 74–6
Plieno CEO, 74–5
transference, 72, 75, 76
threat and vulnerabilities, 68
threat identification, 64–5, 65
vulnerability identification
BigMIMS, 66
BigRX, 67
Pen-testing, 66
scanning results, 66
system administrators, 66–7
qualification risk assessment
acquisition or development, 56
annual loss potential, 63
assets value
loss, estimation
asset value (AV), 61
risk exposure (RE), 61
CEO, 57–8
cyber incidents, 55
intellectual property and trade secrets
acquisition or development, 56
liabilities, 56–7
maintenance costs, 56
profit value, 56
replacement, and costs, 56
risk analysis, 57
unavailable cost, 56
investors and competitors, 57
liabilities, 56–7
loss, estimation
asset value (AV), 61
risk exposure (RE), 61
CEO, 57–8

SLE, 60–62
maintenance costs, 56
profit value, 56
replacement and costs, 56
risk analysis, 57
threat likelihood, estimation, 62–3
unavailable cost, 56

RAT see remote access trojan (RAT)
regulatory communication risk
cybersecurity disclosure, objectives, 83
disclose risks and incidents, reasons, 83–4
reporting mechanisms, 84–5
SEC CF DG 2 guidance
description of business, 82
disclosure controls and procedures, 82–3
legal proceedings, 82
MD&A, 81–2
risk factors, 80–81
SEC investigations, violations, 85–6
SEC regulations
administrative action, 86
civil action, 86
disclosure obligations, 79–80
voluntary disclosure program, 85

Remote Access Policy
anti-virus and anti-malware software, 178
authentication, 178
official business, 177
provision services, 178
training, 178
remote access trojan (RAT), 43, 50, 176, 207–8, 238

Removable Media Policy
automatic scanning, USB ports, 176
disable auto-play, 176
exfiltration of information, 175
media screening capability, 176
nonapproved media, USB ports, 176
in non-organization sources, 177
in organization, 176
risk appetite, 175
Universal Serial Bus (USB) ports, 175
value of information, 175
work force, training, 177
resources, cyber-related
finances, 104
information, 103
personnel, 104
plans, 103, 104
technology, 104
risk appetite level, 91
risk management
boardroom interactions, 326
committees
material enterprise risk, 89
nonmanagement directors, 89
quality decisions, 89–90
technical awareness, 90
threat awareness, 90
CRO, 90–91
cybersecurity risk, 38
human risks, 47–54
insurance, 38
intellectual property and trade secrets, threats, 38–42
internal communications
Critical Information Reporting process, 78–9
Five W’s, 78
metrics, 79
senior management, 78
standardized risk management process, 78
success breeds success, 79
threats and vulnerabilities, 79
qualitative see qualitative risk assessment
quantitative see quantitative risk assessment
regulatory communications see regulatory communication risk
risk decisions, 71–7
shareholders communications, 38, 87–8
technical see technical risk management
threats, 37
router, 30, 62, 207, 278–9, 353

Sarbanes–Oxley (SOX) Act, 82, 193, 201, 246, 263
Securities and Exchange Commission (SEC)
Division of Corporate Finance, 79
security
measures, physical/network, 293–5
memory leakage, 208
patching, 208–9
server, 354
threats and vulnerabilities, 208
server, 40, 44, 45, 59, 73, 159, 161, 164, 187, 203, 207–8, 212, 266, 269, 304, 354
service-level agreements (SLAs), 206, 209
ShadowCrew, 22
shareholders communications
  crisis, 87–8
  information, 87
  preferences, 87
  SEC reports, 86
  stockholder meetings, 87
shareware, 184
SLAs see service-level agreements (SLAs)
SMART (specific, measurable, achievable, realistic, and timely) goals, 124, 132
sniffer, 23
social engineering, 35, 49, 52, 66, 148, 244, 349
software bloat, 208
software license, 105, 182, 184
Software Policy
  acquisition, 183
  applicability, 183
  auditing, 183
  budget, 183
  copying and distribution, 184
  on home systems, 184–5
  inventories, 183
  licensing and registration, 183
  shareware and freeware, 184
  software installation, 183
  storage and documentation, 183
  upgrades, 183–4
spam, 53, 87, 141, 157, 174, 187, 244–5, 263, 278, 283
spam filters, 278
spear-phishing, 28, 48, 49, 53, 99, 149, 173, 187, 210, 244, 263, 269, 350–351
spoofing, 251
spyware, 157
SQL injection see structured query language (SQL) injection
strategic planning, 125
strategy
  boardroom interactions, 328
  cybersecurity, 95–7
  definition, 96
  failure see strategy failure, avoiding
  incorporating cybersecurity, 119–20
  leaders, examples, 96
  mechanics see mechanics of strategy
  operational level planning, 122
strategic level planning, 122
and strategic planning, difference, 97
tactical level planning, 122
strategy failure, avoiding
  communication, 113–14
  human element, understanding, 116
  leadership and oversight, lack of, 117–18
  Netflix, example, 111–12
  Operation Edna, example, 116
  poor plans, poor execution, 111–12
  resistance to change, 114–16
  strategies, implementation, 117
Structured Query Language (SQL) injection, 129–33, 135, 140, 187, 211
BigRX Plan, 135–9
  reducing BigRX’s exposure, 129–30, 133–4
Stuxnet, 17, 40, 43, 47, 75, 175, 250, 253, 255
substandard products and services
  Boeing 787 Dreamliner, 31
  counterfeit products, use of, 30
  cyber threat sources, 12, 36
  help desks, 34–5
  loss, business, 34
  outsourcing, 35–6
  recognizing, 29–30
  smart systems and sensors, 32
  social engineering, 35
  technology, 33
Supervisory Control and Data Acquisition (SCADA) systems, 47
switch, 76, 220, 285, 302–3, 305
SWOT analysis
  opportunities
    data sharing, 102
    partnerships, 102
    payments, 102
    presence, 101
  strengths
    information, 99
    plans, 100
    policies, 100
    presence, 99–100
    processes, 100
    resources, 100
    talent, 100
    technology, 100
  threats
    benchmarking, 103
    standards, 103
technology changes, 103
weaknesses
priorities, 101
resources, 101
risk analysis, 101
third-party assessment, 101
tail-gating (drafting), 170
team creation
business and employees, 229
cybersecurity leaders
business processes, 236
CIOs and CISOs, 233–4
CISSP and CISM certifications, 234–5
CRO and CSO, 236–7
C-suite, 236
cyber smart, 237
technical staffs, 236
Kolb, Jon, 230
long snappers, 229–30
right leaders
attitudes, 231
bad reputation, 231
cyber smart, 233
e-commerce, 232
education, 232
information-enabled activities, 230–231
professional career, 230
safeguard, 231–2
slick salesman’s, 232
technical experts, 231
team selection, 131–2
technical risk management
common technical risks (checklist)
cloud, storage, 44–5
hacking, previous incidents, 43
malicious code, 43
mobile devices, 45
passwords, 45
probing, 43–4
software currency, 44
passwords
practices, 45–6
remote access, 46–7
vulnerability scans, 46
Technology Disposal Policy
construct (model), categories, 160
enforcement, 161
financial or logistics department, 161
information, categories, 159–60
PII disclosure, 158
printers and copiers, 160–161
risk management program, 159
THAAD system, 158
Ten Commandments of Computer Ethics, 143–6
Terminal High Altitude Area Defense (THAAD) system, 158
threat
awareness, 90
detection
phishing messages, 278
quantitative measure, 278, 279
repeat offenders, charts, 277–8, 279
reverse lookup, 279
scans and probing, 277–8
spam filters, 278
identification, 64–5, 65
incident analysis, 188
insider
cyber threat sources, 12, 36
definition, 26–7
example, 28
spear phishing, 28
mercenary hackers, 21
nation-state see nation-state threats
risk management, 38–42
sources, 12, 36, 55, 64, 68, 74, 78, 85
SWOT analysis see SWOT analysis
and vulnerabilities, 68, 79, 208
Time Warner, 126
training
employee
accomplishment, 246
CEO client, 243
certification/decertification, 246
common mistakes, 245
computer safety, 242
cybersecurity and risk management, 243–4
ethics, 246
foot stompers, 244–5
home and office, protection, 245–6
mistake, organizations, 243
principles and techniques, 242
privacy, 244
procedures, 244
purpose, 243
training (cont’d)
executives
  computer crime, 247
decision-making processes, 246
ethical behavior and business practices, 247
globalization and Internet, 248–9
intellectual property and trade secrets, 248
legal and regulatory requirements, 246–7
privacy and anonymity, 247–8
Sarbanes–Oxley Act, 246
violation, 247
trojan, 42, 43, 254
trusted relationships, 318
trustworthy computing, 105
Twitterverse, 26
two-factor access procedures (dual factor)
  authentication, 45, 178, 352–3, 355

uninterruptible power supply (UPS), 163
Universal Serial Bus (USB) ports, 39, 175
Unrestricted Warfare, 13
UPS see uninterruptible power supply (UPS)
U.S. Department of Homeland Security (DHS), 7, 52, 62
values, 107
virtualization, 203
virtual machine (VM), 134
virtual private network (VPN), 23, 354
virus, 43, 46, 54, 103, 175–7, 238, 250, 253, 269, 281, 303, 350
vision, 105–6
vision statement, 107
VM see virtual machine (VM)
voice over Internet protocol (VOIP), 21

VOIP see voice over Internet protocol (VOIP)
VPN see virtual private network (VPN)
vulnerability(ies)
  beyond projected life span, 280
dashboards see vulnerability(ies)
discovered on systems, 279–80
identification
  BigMIMS, 66
  BigRX, 67
Pen-testing, 66
scanning results, 66
system administrators, 66–7
management, 187
passwords, scan, 46
residual, 280
scanning, 138
SQL injection, 68, 129, 133, 135
system, 279
threats and, 68, 79, 208, 228
time frames, 280

war driving, 23
web pages
  Cross-Site Scripting (XSS), 211–12
digital storefront, 212
products and services, advertise, 202
United Airlines, 212
ZNews Network, 211
whaling, 28, 48, 244
white listing, 187
wireless devices, 354–5
worm, 42, 43, 49, 103, 176
  zero-day, 216, 290
zero tolerance, 146
ZNews Network, 211
zombie, 60, 176, 200, 302
zone locations, 204