Index

#
2-factor authentication, 57, 295, 296
9/11/2001. *See* September 11, 2001
60-Day Cyberspace Policy Review, 100–101, 130, 259
256-bit encryption, 193
300A and 300B reports, 170
414s (hackers), 6
1930s IT infrastructure, 185
1940s IT infrastructure, 75
1950s IT infrastructure, 75–76, 185¬
1960s cybersecurity issues, 4, 76–77, 95
1970s cybersecurity issues, 5, 179
1980s cybersecurity issues, 4–9, 77–81, 82, 185
1990s cybersecurity issues, 9, 81–90, 223–225, 276
2000s cybersecurity issues, 9, 89, 90–101, 220, 276
2010s cybersecurity issues, 10, 101–104, 221–222, 276

A
A circulars. *See under* OMB
AC (actual cost), 152–154, 156, 299–300, 302
acceptable levels of risk, 36
acceptable quality level (AQL), 145
accepting risks, 16, 20, 22, 60–61
access codes, 236
access points, 233, 258
accessibility of systems
  corporate systems, 233
  health care systems, 224
  mainframe computers, 76
  network access points, 233, 258
  physical sites, 236
  vs. security, 22
account number access, 273
accounting, 148–149, 230
accounting machines, 185
accreditation (IT systems), 171–172
accuracy of warnings, 112
acquisition program baseline (APB), 142
acquisitions and procurement
  acquisition documents, 143–148
  acquisition phase, 143–148
  Brooks Act, 76–77
  CIOs and, 83–84
  compliance, 168–169
  GSA and, 77
  OMB and, 82, 83–84
  Paperwork Reduction Act, 82
  supply chain security, 166, 170
active responses to threats, 207–208, 237–238
acts of law, 263
actual cost (AC), 152–154, 156, 299–300, 302
ACWP (actual cost of work performed), 152
"adequate security," 171
Administrative Procedure Act (APA), 266
advanced notices of proposed rulemaking (ANPR), 260, 266
advanced persistent threats (APTs), 203–204, 276, 277
Advanced Research Projects Agency (ARPA), 4
Advanced Research Projects Agency Network (ARPANET), 4, 179
African Network Information Centre (AfriNIC), 278
agencies
  audits, 241
  budgets, 260
  civilian. *See* civilian agencies
  classified/unclassified protective markings, 79
  compliance standards, 168–169
  creation of, 266
  cybersecurity policy role, 69–70
  Federal Register rules publication, 260
  FISMA requirements, 97–98, 171
  impact on projects, 123
  intelligence. *See* intelligence agencies
  inter-agency cooperation, 87
  military. *See* Defense Department
  operational planning model, 124
  procurement responsibilities, 83
  public hearings, 266–267
  public-private partnerships. *See* private-public partnerships
  regulations, role in, 265–268
  regulatory agencies, 265–266
  supervision of, 74
  top-down analysis, 50–52
aggravated identity theft, 273
agriculture as critical infrastructure, 96
"ahead of schedule" variances, 155, 298–299
Air Force, 71, 72
alerts
  as cybersecurity capability, 203, 207

as high-level requirement, 136
National Cyber Alert System, 94
trusted Internet connections example, 139
warning systems, 110–113, 122–123, 136, 203, 207
Allen, William T., 217
alternative hypotheses (H_a), 39, 49, 291
alternative scenarios, 119–120, 138
ambiguity in survey design, 288
amendments, bills, 262, 263
American Recovery and Reinvestment Act, 225, 241
American Registry for Internet Numbers (ARIN), 278
analyzing threats, 104, 136, 203, 206–207
Anil, Suleyman, 101, 283
anomalies
corporate detection, 237–238
DHS monitoring case study, 162–163
network detection, 203, 206
simulating, 206–207
anonymity, 279, 281
Anonymous, 19
ANPR (advance notice of proposed rulemaking), 260, 266
Antarctica, 278
Anti-Referral Payments Law, 217
antivirus software
corporate obligations and, 220
informing internal information, 162
in internal monitoring, 205
McAfee, 115
TJX data breach and, 227
as warning system, 207
APA (Administrative Procedure Act), 266
APB (acquisition program baseline), 142
APNIC (Asia-Pacific Network Information Centre), 279
appeals and appeals courts, 268
APT (advanced persistent threat), 203–204, 276, 277
AQL (acceptable quality level), 145
ARIN (American Registry for Internet Numbers), 278
Army, 71, 72
ARPA (Advanced Research Projects Agency), 4
ARPANET (Advanced Research Projects Agency Network), 4, 179
arraignments, 274
Asia, 279
Asia-Pacific Network Information Centre (APNIC), 279
assembly language, 180–181
assessing plans, 120
assessing results, 120–121
assessing risks. *See* risk assessments
assessing threats. *See* threat assessment
assets
capital, 149, 150, 169–170
corporate, 234
critical, 31–33, 61
FISMA compliance, 170–172
GAO labeling system, 31–33
identifying, 160–161
assistance as high-level requirement, 136
assistant to the president for homeland security and counterterrorism, 100
assumptions
risk determination and, 33
in risk management framework, 16, 20, 21
spear phishing survey, 42
in survey design, 288
asymmetrical warfare, 6
"at rest" encryption, 194
atomic bombs/nuclear arms, 6, 7
atomic energy. *See* nuclear facilities
attachments (email), 195, 235
attacks and exploits, 195–196
active/passive responses, 207–208, 237–238
alerts. *See* alerts
anomalies and, 162–163, 203, 206–207, 237–238
BGP, 191–192
botnets, 198
brute force, 193
buffer overflow, 201
code injection, 201
crashing and recovery, 201
data breaches. *See* data breaches
denial of service, 198, 203, 204, 275
DHS monitoring case study, 162–163
DNS cache poisoning, 200
factors aiding in, 202
growth in 2000s, 99
history of, 275–276
insider threats, 200, 233
malware, 195, 196, 271
man in the middle, 198–199
phishing/spear phishing, 41–46, 197–198
private sector breaches, 213
private sector plans, 211–212
SEC disclosures, 229
simulating, 206–207, 234–235
threat signature technology, 99–100
time before discovery, 281
types of, 187
unknown vulnerabilities, 201–202
warnings. *See* warning systems
zero-day exploits, 201–202
attribution for attacks, 190, 195, 281

audits, 240
agencies, 241
corporate policies, 239–241
financial, 167
FTC consent agreements, 226
health care systems, 173, 224
internal/external, 166–168, 239–241
IT, 167, 173
monitoring functions and, 204
risk assessment, 240
Sarbanes-Oxley Act, 230
technical, 167
types of, 166–168
Australia, 279
authentication tokens, 213
authority, transnational, 281–282
authorization, 133, 134–135, 139
automatic alert systems, 112
Automatic Data Processing Act (Brooks Act), 76–77, 80, 83
availability, threats to, 187
avoiding risks, 16, 20, 60, 61
awareness campaigns, 207, 224
Azerbaijan, 277

B
BAC (budget at completion), 157, 300, 301, 302
back-ups, off-site, 236
backbones, 4, 188
backwards engineering (op models), 141
badges, 236
bail, 274
bandwagon fallacy, 249
banking and finance systems
criminal information access, 271, 273
as critical infrastructure, 86, 87
cyber threats, 87
Estonian attacks, 101
GLB Financial Modernization Act, 222–223
Sarbanes-Oxley Act, 168, 230
TJX breach losses, 220, 226–227, 272
written security plans, 223
baselines, establishing, 160–161, 171
BCWP (budgeted cost of work performed), 153
BCWS (budgeted cost of work scheduled), 152
behavioral detection, 206, 233
"behind schedule" status, 163, 298–299
best practices, 103, 304
BGP (Border Gateway Protocol), 187, 188, 190–192, 198–199
biases, 288, 289
big picture, senior managers and, 115, 116
bills, legislative, 261–263
binary code, 180, 193
binary dependent variables, 292
BJR (business judgment rule), 219
Black Hand, 276
black hole servers, 204
blackouts, 92
"Blueprint for a Secure Cyber Future," 130, 259
boards of directors
business judgment rule, 219
duty of care, 215–219
liability, 218
obligations, 221–222
role in company, 214
role in cybersecurity, 211–212, 214, 231–232
as senior managers, 110
Border Gateway Protocol (BGP), 187, 188, 190–192, 198–199
botnets, 198
bottom-up assessments (PWS), 145
Bottom-Up Review report (BUR), 130, 259
boy genius hackers, 5–6, 27
brokerage firms, 228
Brooks, Jack, 76
Brooks Act, 76–77, 80, 83
brute force attacks, 193
budget at completion (BAC), 157, 300, 301, 302
budgeted cost of work performed (BCWP), 153
budgeted cost of work scheduled (BCWS), 152
budgets
APBs, 142
comparing projects, 157–158, 298–302
congressional control, 74
CONOPS and, 138
as constraints, 21
developing, 120, 149–152
EVM development of, 149–152
EVM indexes, 298–302
EVM management, 148
manager's role, 117
OMB control, 84
over or under status, 156
in proposed legislation, 262
trade-offs in risk management, 23
understanding, 150–152
buffer overflow attacks, 201
bulk power systems, 229–230
BUR (Bottom-Up Review report), 130, 259
Bureau of the Budget. *See* OMB (Office of Management and Budget)

Bush administration
CNCI founding, 99–101
critical infrastructure directives, 95–97
E-Government Act, 97–98
Executive Orders, 257
FISMA act, 97–98
Homeland Security history, 90–99
HSPDs, 95-97
national security instruments, 255
presidential power expansion, 129–130
Sarbanes-Oxley Act, 168, 230
business continuity plans, 238
Business Corporation Law of New York State (NY BCL), 216
business interruption insurance, 238
business judgment rule (BJR), 219
businesses. *See* private sector
bylaws, corporate, 214

C
C++, 181
CAATs (computer-assisted audit techniques), 167
cable companies, 188
cache, 184
cache poisoning, 200
California
    data breach laws, 227–228
    electrical grid attacks, 276
cameras, activating, 102
Canada, 278
capabilities
    capability-based planning, 136–137
    capability gaps, 133–134, 135, 137, 139
    CONOPS, 137–140
    defining for monitoring systems, 159
    examples, 26–27, 202–208
    identifying for threat assessment, 25
    identifying in PWSs, 145
    mission needs statements, 133–134
    op models, 141
    organizational needs, 118–119
    translating goals into, 114
capability-based planning, 136–137
capability gaps, 133–134, 135, 137, 139
capacitors, 185
capital, 109
Capital Asset Plan and Business Case (Exhibit 300), 169–170
capital assets, 149, 150, 169–170
Caremark International lawsuit, 216–219
Caribbean region, 278, 279
catastrophes. *See* disasters
"catastrophic" label (GAO), 31–33
causation *vs.* correlation, 57
CD-ROM drives, 182
CDs, 185
Central Asia, 279
Central Intelligence Agency. *See* CIA
central processing units (CPUs), 181
CEOs (chief executive officers)
    business judgment rule, 219
    cybersecurity role, 211–212, 215, 232
    duty of care, 215–219
    liability, 218
certificates (HTTPS), 194
certification (IT systems), 171–172
"CF Disclosure Guidance: Topic No. 2," 229
CFAA (Computer Fraud and Abuse Act), 8–9, 270–272
CFR (Code of Federal Regulations), 172, 268
challenge questions, 295, 296
changes, identifying
    evolution of threats, 105
    in file data, 195
    monitoring risks, 62–63, 64
    risk management framework, 16, 20
charging criminals, 274
Charter Pacific Bank, 222
charters, corporate, 214
Chechnya, 276
checklists, going beyond, 66
chi square test, 291
chief executive officers (CEOs), 211–212, 215–219, 232
chief information officers. *See* CIOs (chief information officers)
Chief Information Officers Council (CIO Council), 84, 256
chief information security officers (CISOs), 232
chief infrastructure assurance officers (CIAOs), 89
child prodigy hackers, 5–6, 27
China, 37, 276
CIA (Central Intelligence Agency), 72, 73, 77, 90, 91
CIAO (Critical Infrastructure Assurance Office), 89, 94–95
CIAOs (chief infrastructure assurance officers), 89
CICG (Critical Infrastructure Coordination Group), 87
CIKR (critical infrastructure and key resources), 97. *See also* critical infrastructure
CIO Council, 84, 256
CIOs (chief information officers), 59
    business judgment rule, 219
    cybersecurity role, 83–84, 211–212, 215, 232
    duty of care, 215–219

FISMA compliance, 171
liability, 218
CISOs (chief information security officers), 232
Citigroup, 218–219
citizen concerns, military information control, 80
civilian agencies
Brooks Act responsibilities, 77
capability-based planning, 136–137
CONOPS, 137–140
cybersecurity role, 69–71, 73
DHS as, 95
Einstein 3 monitoring, 100
EVM accounting and, 148
FISMA requirements and, 98
mission needs statements, 126–127
national cybersecurity threats management, 8
op models, 140–142
tensions with military, 70, 71, 78–81, 104–105
CIWG (Critical Infrastructure Working Group), 86
claims processors, 225
classified information
CNCI declassification, 101
criminal information access to, 270
document markings, 79
early cybersecurity policies, 8
NSA classified computer systems, 80
NSA SBU IT, 81
personal computer security, 78
classified technology, 81
Clinger-Cohen Act of 1996, 83–84, 126, 168–169
Clinton administration
CIO Council, 84
cybersecurity and terrorism, 85–90
executive orders, 256
national security instruments, 74, 86–90, 255, 261
Presidential Decision Directives, 74, 86–90, 255, 261
Y2K preparations, 89
closed-ended questions, 288
cloud providers, 202, 219–222
CMS (continuous monitoring system), 122–123
CNCI (Comprehensive National Cybersecurity Initiative), 111
history of, 99–102
mission requirements in, 130
partial declassification, 101, 257
TIC initiative, 258
warnings capability, 110
Coast Guard, 71
Coast Guard Intelligence, 72
COBIT (Control Objectives for Information and Related Technology), 239–240
code breaking agencies. *See* NSA
code injection, 201
Code of Federal Regulations (CFR), 172, 268
coefficient of determination, 292
Cold War, 3–4, 76, 78
collaboration, as high-level requirement, 136
color-coding project status, 165
.com domains, 192
command and control attacks, 196
commenting on proposed rules, 266
Commerce Department, 77, 89, 98, 278
Committee of Sponsoring Organizations (COSO), 239
committees, congressional, 262
communication pathways, 185, 240–241. *See also* networks
communication systems, 85, 87, 96
communications, intercepting, 272. *See also* attacks; data breaches
companies. *See* private sector
completion dates (POA&M documents), 147–148
compliance, 167
audits, 166–168
compliance officers, 167
corporate employees, 235
Exhibit 300, 169–170
federal CIOs role, 84
federal practices, 168–169
FISMA requirements, 170–172
HIPAA example, 172–174
internal controls, 239–240
monitoring risks, 62–63, 64, 204
noncompliance consequences, 172
operational planning model, 125
operational requirements documents, 140
post-breach reports, 237
risk management framework, 16, 20
"Compliance and Reporting" block, 125
compliance officers, 167
components (hardware), 181, 182–183
Comprehensive National Cybersecurity Initiative. *See* CNCI
compromised systems, 195
computer-assisted audit techniques (CAATs), 167
Computer Fraud and Abuse Act (CFAA), 8–9, 270–272
Computer Readiness Team (US-CERT), 94, 122–123, 259
computer science, 179–180
Computer Security Act of 1987, 79, 80–81
computers, 180
attacks and exploits. *See* attacks
cryptographic technologies, 193–195

cybersecurity operation capabilities, 202–208
federal standards for, 169
history of, 179
mainframes, 75–76
memory, 184–185
multiple processors, 182
personal computers. *See* PCs
processors, 181–182
procurement. *See* acquisitions and procurement
programs, 181–182
protected, 272
research systems, 4
as systems, 182–184
vulnerabilities, 200–202
Concept of Operations (CONOPS), 137–140
conditional events (probability), 48–49
conference committees, 263
confidence intervals (statistics), 291
confidential information. *See* classified information; customer information; personal information
confidentiality breaches, 187
configuration, network, 201, 237
Congress
agency creation, 266
agency supervision, 74
authority, 260
Congressional Research Service, 264–265
cybersecurity policy role, 69–70
federal regulations, 265–268
GAO information, 264
legislation process, 261–263
military/civilian security control policies, 71
mission requirements, 127, 128
power of the purse, 260
proposed bills and law research, 264
research sources, 250–251, 264
response to NSDD-145, 80–81
as senior managers, 110
Congressional Record, 263, 264
Congressional Research Service (CRS), 264–265
CONOPS (Concept of Operations), 137–140
consent agreements, 226, 227
consequence assessments, 30–33
in consequence equation, 31
DHS monitoring case study, 161–162
metrics, 33
model corporate cyber program, 232, 234
consequences, 23, 30
analyzing threats/vulnerabilities, 33–37
assessing. *See* consequence assessments
assigning values to, 35–37
in consequence equation, 31
corporate governance and, 216
direct/indirect, 30
identifying, 38
illustrated, 38
increases in, 33
metrics, 33
in PRA risk management, 47
in risk assessment, 23, 47
in risk determination, 36
in risk equation, 23
in risk management framework, 16, 20
Constitution, 250, 251, 262, 268
constraints
in CONOPS, 137–140
identifying, 140
internal/external, 123
in risk management framework, 16, 20, 21–22
user-friendly websites and, 58, 59
containing threats
as capability, 203
"contain" task in risk management, 15
corporate policies, 237
risk responses, 61
continuity plans, 238
continuous monitoring system (CMS), 122–123
contracting officers, 146–147
contractors. *See* vendors/contractors
contracts, 238
control activities (businesses), 240
control environments (businesses), 240
Control Objectives for Information and Related Technology (COBIT), 239–240
convenience sampling, 289
Convention on Cybercrime, 284
coordination role (management)
failures of, 123
functions, 115–117
as high-level requirement, 136
managing *vs.* doing, 113–114
Coreflood virus, 198
Corporate Finance Division (SEC), 228
corporate governance, 213–215
corporations. *See* private sector
correlation *vs.* causation, 57
COSO (Committee of Sponsoring Organizations), 239
Cost Performance Index (CPI), 157, 299–300, 301, 302
cost variances (CVs), 155–158, 163–164
costs
attack simulations, 235
in budgets, 150–152

cost variances, 155–157, 163–164
data breaches, 9, 220, 221, 229, 236
DHS monitoring case study, 160–161
District Design case study, 151–154
IGCE estimates, 146–147
objective and threshold values, 142–143
op models, 140–142
Sony PlayStation breach, 221
TJX data breach, 220
worm damage estimates, 9
Council of Europe, 284
counterintelligence, 99–102, 281. *See also* espionage; intelligence agencies
counterterrorism review of policies, 100–101
courses of action, 135. *See also* plans; strategies
Court of Appeals, 268
courts
international, 282
U.S. *See* judicial branch of government
CPI (Cost Performance Index), 157, 299–300, 301, 302
CPU (central processing unit), 181
credit and debit cards
criminal information access, 273
liability for breaches, 219–222
personal information sales, 222
prosecutions for breaches, 272
Sony PlayStation Network breach, 221–222
TJX data breach, 220, 226–227, 272
credit reporting agencies, 228
criminal acts. *See also* attacks; data breaches
Computer Fraud and Abuse Act, 270–272
Federal crimes, 269–270
federal prosecution process, 273–275
identity theft, 219, 270, 271, 273
international issues, 282
Wiretap Act, 272
criminals. *See* hackers; nation-state hackers; organized crime groups
crisis management, DHS role in, 95
critical assets
consequence assessments, 31
GAO labeling system, 31–33
removing, 61
"Critical Foundations: Protecting America's Infrastructures," 86–87
Critical Infrastructure Assurance Office (CIAO), 89, 94–95
critical infrastructure components, 85. *See also* critical infrastructure protection
agriculture, 96
banking and finance systems, 86, 87
blackouts, 92
CIKR (critical infrastructure and key resources), 97
communication systems, 85, 87, 96
electrical grid, 85, 87
emergency services, 87
Energy Department management, 96
food systems, 96
identifying critical infrastructure, 95–97
Internet, 275
in policy formation, 74
power plants, 229–230
private sector ownership, 85
sectors of, 96
transportation systems, 85, 87, 96
water systems, 87, 96
Y2K preparations, 89
Critical Infrastructure Coordination Group (CICG), 87
"Critical Infrastructure Identification, Prioritization, and Protection," 95–97
critical infrastructure protection. *See also* critical infrastructure components
board of directors role, 231–232
CIWG review, 86
corporate policies, 235
Critical Infrastructure Assurance Office, 89
Critical Infrastructure Protection Board, 92–93, 257
Critical Infrastructure Working Group, 86
Cybersecurity Act of 2012, 103
DHS responsibilities, 18, 90–91, 93–95, 96, 97, 104
executive orders. *See* EOs
National Coordinator for Security, Infrastructure Protection and Counter-Terrorism, 88
National Infrastructure Advisory Council, 93
National Infrastructure Assurance Council, 87
National Infrastructure Protection Center, 89–90, 94–95, 261
National Infrastructure Protection Council, 93–94
National Infrastructure Protection Plan, 18, 87, 94, 96, 97, 104
National Policy for Infrastructure Protection, 87
NSC (National Security Council), 87, 93
Office of Infrastructure Protection, 94, 131
Office of National Infrastructure Assurance, 87
national security instruments. *See* national security instruments
policies, 74, 87–90
President's Commission on Critical Infrastructure Protection, 86–87, 255, 256
private sector ownership, 85, 105
public-private partnerships, 70, 85, 87–88, 105
sentencing and, 275

Y2K preparations, 89
Critical Infrastructure Protection Board, 92–93, 257
Critical Infrastructure Working Group (CIWG), 86
"critical" label (GAO), 31–33
criticality, defined, 31
CRS (Congressional Research Service), 264–265
cryptographic technologies, 193–195
cryptological agencies. *See* NSA
CS&C (Office of Cybersecurity and Communications), 94, 122, 131
customer information
banks selling, 222
business's duty towards, 212–213
criminal access to, 271, 273
FTC and, 225–228
leak example, 55–60
Sony PlayStation Network, 221–222
statistical models for risk, 292–296
TJX data breach, 220, 226–227, 272
CVs (cost variances), 155–158, 163–164
Cyber Defense Policy (NATO), 283
cyber intrusions, defined, 195
"Cyber Security Incident Reporting and Response Planning," 230
cyber security incident response plans, 230
cyber warfare
Estonia, 101
history of, 275–276
Olympic Games program, 102
UN and, 283
cybersecurity. *See also* computer science; federal government; legislation; policies; private sector; research; risk management
capabilities, 202–208
facets of, 11–13
global issues in, 275–284
history of issues, 3–10
model corporate framework, 231–238
risks in cyberspace, 15–17
Cybersecurity Act of 2012, 102–103
cybersecurity coordinator (White House), 101, 103, 259
cybersecurity insurance, 61–62
cybersecurity management framework
best practices, 125
capability-based planning, 136–137
civilian agencies, 136–142
congressional/presidential input, 128–131
CONOPS and op Models, 137–142
DHS framework, 125–126
high-level requirements, 132–136
mission needs statements, 126–127, 132–136
objective values, 142–143
sector differences, 127
cybersecurity managers. *See* program/project managers
cybersecurity operation capabilities, 202–208
Cyberspace Policy Review, 100–101, 130, 259
cyclical nature of management, 121

D

damages
attacks, 196
business data breaches, 212
examples, 26–27
identifying in threat assessment, 25
lethality, 25, 26–27
mitigating, 237
model corporate cyber program, 232
risk tolerances, 22
data, 180
analyzing traffic, 206–207
backing up, 236
business transactions, 212–213
cryptographic technologies, 193–195
encryption, 235–236
monitoring, 203–205
packet analyzers, 204
removal/exfiltration, 196
data breaches
business implications, 212–213
costs of, 9, 220, 221, 229, 236
Federal Trade Commission and, 225–228
HIPAA, 223–225
international issues, 282
liability for, 219–222
notifications, 236–237
sentencing penalties, 275
Sony PlayStation Network, 221–222
TJX case study, 220, 226–227, 272
types of violations, 187
databases, 212–213
DCA (Defense Communications Agency), 4
DDoS attacks (distributed denial-of-service), 10, 198
DEA (Drug Enforcement Administration), 72
deadlines, project, 135
debit cards. *See* credit and debit cards
decision-making process, 117–121
declassification of CNCI, 101
decryption, 193
defense, as high-level requirement, 136
Defense Communications Agency (DCA), 4
Defense Department
agencies and commands, 71–73

ARPANET, 4
CNCI directives, 99
computer procurement, 77
FISMA and, 98
on Homeland Security Council, 91
ISAC participation, 90
managing national cybersecurity threats, 8
planning, programming, budgeting and execution, 127
WBS budgeting, 150
Defense Information Systems Agency, 4
Defense Intelligence Agency (DIA), 72
Delaware Court of Chancery, 217, 219
Denial of Service (DoS) attacks, 198, 203, 204, 275
departments of government. *See* names of specific departments (Defense Department, DHS, EPA, etc.)
dependent variables (modeling), 56, 292, 293, 294
dependent variables (research), 247
descriptive research, 248
detailed technical guidance, 304
detection, as high-level requirement, 136
DHS (Department of Homeland Security)
agencies collected under, 93–95, 131
capability-based planning, 136–137
Critical Infrastructure Protection Board, 93
cybersecurity agencies in, 94
cybersecurity management framework, 125–126
cybersecurity policies, 97
cybersecurity reports, 130–131
DHS Risk Lexicon. *See* DHS Risk Lexicon
EVM systems, 148, 158–164
expanded scope of government and, 129
FISMA and, 102–103, 258
founding of, 90–91
guidance statements, 130
infrastructure protection, 93, 104
military and intelligence agencies, 71–73
mission needs statements, 130–131, 133
monitoring system case study, 158–164
National Infrastructure Protection Plan, 18, 96, 97
"National Strategy to Secure Cyberspace," 95
National Vulnerability Database, 201
program managers, 127
Strategic Plan, 259
structure of, 131
TIC mandate, 258
warning systems challenges, 112
DHS Risk Lexicon
consequences, 30
game theory, 56
likelihood, 37
risk assessment, 23
risk transfer, 61
threat shifting, 28
threats, 25
vulnerabilities/vulnerability assessments, 29
DIA (Defense Intelligence Agency), 71
Digital Equipment Corporation, 5
digital signatures (domains), 192
direct consequences, defined, 30
direct relationships (logit models), 56
directives
defined, 304
presidential. *See* presidential directives
disasters
"catastrophic" label, 31–33
risk management models and, 17
threats resulting from, 233
as unintentional threats, 26
disclosures, 228–229, 237
disjoint events (exclusive events), 48–49
disseminating information, as capability, 159
distributed denial-of-service attacks (DDoS), 10, 198
distribution attacks, 196
district courts, 268
District Design case study
budgeting, 149–154
cost variances, 156–157
EVM indexes, 298–302
introduction, 149
schedule variances, 155, 158
division (voting), 263
DNS cache poisoning, 200
DNS (Domain Name System), 188, 192, 277, 278
DNSSEC (Domain Name System Security Extensions), 192
document classification, 79
"doing," *vs.* managing, 113–114
domain name registries, 192
Domain Name System (DNS), 188, 192, 277, 278
Domain Name System Security Extensions (DNSSEC), 192
DoS (denial of service), 198, 203, 204, 275
downloading files, 235
drones, 276
Drug Enforcement Administration, 72
duty of care, 215–222, 238
DVDs, 185

E

E-Government Act of 2002, 97, 171
EA (enterprise architecture), 169
EAC (estimate at completion), 157, 301–302
Earned Value. *See* EV (earned value)

earned value management. *See* EVM (earned value management)
ecological fallacy, 249
economic incentives, 87, 103, 145
EDGAR (Electronic Data Gathering, Analysis, and Retrieval), 229
.edu domains, 192
educating users. *See* training
effective dates (regulations), 267
effectiveness
  monitoring risks, 62–63, 64
  risk management framework, 16, 20
  warning systems, 112
Einstein 3 program, 99–100, 101
Eisenhower administration, 3–4
electrical grid
  California attacks, 276
  as critical infrastructure, 85, 87
  damage and consequences, 32
  Northeast Blackout, 2003, 92
  power plants, 229–230
Electricity Sector Information Sharing and Analysis Center (ES ISAC), 230
Electronic Communications Privacy Act, 270, 272
Electronic Data Gathering, Analysis, and Retrieval (EDGAR), 229
electronic voting systems, 263
email
  attachments, 195, 235
  corporate policies, 235
  phishing attacks, 41–46, 197–198
  testing vulnerability to, 41–46
  threats to, 87
  as vulnerability, 200
EMC Corporation, 212–213
emergency corporate policies, 237
emergency services, 87, 224
Emerging Security Challenges Division (NATO), 283
employees, 200, 233, 235. *See also* users
encryption
  corporate data, 220, 235–236
  methods, 193–194
  NSA responsibilities, 73
  Sony PlayStation breach, 221
  TJX data breach, 227
  websites, 194
Energy Department, 72, 87, 96
energy systems, 87, 96, 229–230. *See also* electrical grid
enforcement of law and regulations, 269
Enron, 168, 230
enterprise architecture (EA), 169
enterprise risk management (ERM), 239
"Enterprise Risk Management-Integrated Framework," 239
enterprise servers, 185
Environmental Protection Agency (EPA), 47
EOP (Executive Office of the President)
  information management functions, 82
  National Security Council, 253
  OMB role, 253–254
  OSTP technical advice, 254, 259
  research sources, 254
    executive orders, 256–258
    Federal Register, 259
    OMB memoranda, 258–259
    OSTP memoranda, 259
    national security instruments, 255
    White House strategy/guidance, 259
  structure of, 252–253
EOs (executive orders), 256–257, 304
  as authorization, 134
  Bush post-9/11 orders, 90–93, 257
  Clinton's infrastructure protection, 86–87, 256
  EO 13010 (PCCIP), 256
  EO 13011 (CIO Council), 256
  EO 13228 (Homeland Security), 90–91, 257
  EO 13231 (Cyberspace Security), 92–93, 257
  EO 13636 (Critical Infrastructure), 104, 256
  Federal Register listing, 260
  functions of, 74, 256–257
  mission requirements and, 127–130
EPA (Environmental Protection Agency), 47
epistemology, 247
equations
  consequence equation, 31
  Cost Performance Index, 299–300
  cost variances, 155–157
  estimate at completion, 157, 301–302
  estimate to complete, 300, 301
  logistic regression equation, 294, 295
  logit model, 292
  risk equation, 23–25, 34–35
  Schedule Performance Index, 299
  schedule variances, 154–155
  total risk equation, 35
  variance percentages, 157–158
ERM (enterprise risk management), 239
errors
  of omission, 26
  survey design, 288–290
ES ISAC (Electricity Sector Information Sharing and Analysis Center), 230
espionage
  attribution, 281

corporate, 233
early network threats, 4, 5
Flame worm, 102, 276
monitoring for, 204
in threat spectrum, 28
estimate at completion (EAC), 157, 301–302
estimate to complete (ETC), 157, 300, 301, 302
Estonia, 101, 275, 276, 283
ETC (estimate to complete), 157, 300, 301, 302
ethical hackers, 208
Europe, 279, 283, 284
European Network and Information Agency, 37
EV (earned value)
cost variances, 156
CPI equations, 299–300
District Design case study, 152–154
EAC equations, 302
ETC equations, 300, 301
as percentages, 157–158
schedule variances, 154–155
SPI equations, 298–299
evaluation criteria (RFPs), 146–147
event tree analysis, 49–52
events in probability analysis, 48–52
evidence, 281
EVM (earned value management), 148–149
budgets, 149–152
comparing projects, 157–158
DHS monitoring system case study, 158–164
forecasting, 300–302
indexes, 298–302
primary metric breakdown, 153–154
red, yellow, and green status, 165
tracking projects (variances), 154–157
variances as percentages, 157–158
work breakdown structure, 146, 148, 160
EVM forecasting, 300–302
EVM indexes, 298–302
EVM primary metric breakdown, 153–154
exclusive events (probability), 48–49
executive branch of government, 251–252. *See also* presidents
cybersecurity coordinator, 101
Executive Office of the President, 82, 252–260
Federal Register, 260
federal regulations, 265–268
mission requirements, 127, 128–131
policy documents, 254
executive orders, 256–258
OMB memoranda, 258–259
OSTP memoranda, 259
national security instruments, 255
White House strategy and guidance, 259
research sources, 250–251
role in cybersecurity law, 69–70
structure, 252–253
National Security Council, 253
Office of Science and Technology Policy, 254
OMB, 253–254
Executive Office memoranda, 128
Executive Office of the President, 82, 252–260
executive orders. *See* EOs (executive orders)
exfiltration, 196
Exhibit 300 reports, 169–170
experimental research, 247
experts, RFIs and, 143–144
explanatory research, 248
exploits. *See* attacks and exploits
exploratory research, 248
Explorer 1, 3
external audits, 166–168, 240
external constraints, 123
external information gathering, 162
external project information, 119
external risks, 240
external threats, 28
extortion, 272
extrapolation in research, 40

F

F-test, 291
Facebook phishing attacks, 197
failed projects, 122–123
false flagging operations, 281
false positives, 206
FASA V (Federal Acquisition Streamlining Act), 169
fault tree analysis, 50–52, 53, 54
favorable variances, 155, 156, 158, 298, 299–300
FBI (Federal Bureau of Investigation), 72, 90, 91
FDA (Food and Drug Administration), 265–266
FedCIRC (Federal Computer Incident Response Center), 94–95
Federal Acquisition Streamlining Act (FASA V), 169
Federal Bureau of Investigation, 72, 90, 91
Federal Computer Incident Response Center (FedCIRC), 94–95
federal courts. *See* judicial branch of government
Federal Emergency Management Agency (FEMA), 93
Federal Energy Regulatory Commission (FERC), 230
federal government
agencies. *See* names of specific agencies (CIA, FBI, etc.)

Cold War and technology development, 3–4
compliance, 168–169
criminal computer access penalties, 271
cyber attack capabilities, 37
cybersecurity research documents. *See* research sources
departments. *See* names of specific departments (Defense Department, DHS, etc.)
early hackers' threats, 5–6
executive branch. *See* executive branch of government
expanded scope of, 129
growth and information needs, 75
judiciary. *See* judicial branch of government
as largest U.S. information agency, 81–82
legislation, history of. *See* legislation
legislative branch. *See* Congress
managerial roles, 110
military, intelligence, and civilian agencies, 69–73
personal computer security, 77–81
policies. *See* policies (Federal)
regulations. *See* regulations
tensions related to cybersecurity, 70, 71, 78–81, 104–105
Federal Information Security Management Act. *See* FISMA
federal legal system. *See* judicial branch of government
Federal Network Resilience division (FNR), 94
Federal Register, 260, 266
federal regulations. *See* regulations
Federal Sentencing Guidelines, 274–275
Federal Trade Commission Act (FTCA), 226
Federal Trade Commission (FTC), 225–228
FEMA (Federal Emergency Management Agency), 93
FERC (Federal Energy Regulatory Commission), 230
final events (probability analysis), 51
final rules (regulations), 260, 267
final total costs, 300–302
finance systems. *See* banking and finance systems
financial audits, 167
Financial Privacy Rule, 223
"FIPS 200 Minimum Security Requirements for Federal Information and Information Systems," 174
fire hazards, 236
firewalls, 30
corporate networks, 220
DHS monitoring case study, 162
internal monitoring, 205
phishing attacks and, 198
role in cybersecurity, 204
TJX data breach, 227
as vulnerabilities, 30
FISMA (Federal Information Security Management Act)
as authorization, 134
compliance and reporting, 170–172
establishment of, 258
focus on government resources, 97–98
OMB's oversight, 102–103, 129
requirements, 169
scope of, 129
Flame worm, 102, 276
flood hazards, 236
floor debates, 263
FNR (Federal Network Resilience division), 94
focus groups in research, 40
FOIA (Freedom of Information Act), 79
Food and Drug Administration (FDA), 265–266
food systems, 96
forecasting (EVM), 300–302
foreign hackers. *See* nation-state hackers
foreign relations, 270. *See also* global cybersecurity issues
formulas. *See* equations
forward selection (modeling), 294
frameworks, 125. *See also* cybersecurity management framework; risk management frameworks
framing risks, 19
assumptions, 19, 21
constraints, 19, 21–22
illustrated, 16
priorities, 19, 23
risk management and, 20
risk management framework, 16, 17, 18, 19–23
risk tolerance, 19, 22
trade-offs, 19, 23
France's cyber defenses, 37
fraud, 271
fraud scrubs, 222
freedom issues, 282
Freedom of Information Act (FOIA), 79
FTC consent agreements, 226
FTC (Federal Trade Commission), 225–228
FTCA (Federal Trade Commission Act), 226
FTE (full-time equivalent), 160, 161
functions (line and staff), 115–117
"Funding Information Systems Investments," 83
funds. *See* budgets; resources

G

game theory, 55, 56
GAO (Government Accountability Office), 33
asset criticality labeling system, 31–33

capability definitions, 203
functions, 264
internal monitoring tools, 205
proposed federal regulations, 267
US-CERT failure, 122–123
warning notification, 111
gap analysis, 133–134, 135, 137, 139
GB (gigahertz), 182
General Accounting Office. *See* GAO
general counsel (corporate), 211–212
General Services Administration. *See* GSA
genetic fallacy, 249
Georgia, 277
German cyber defenses, 37
gigahertz (GB), 182
GLB Financial Modernization Act, 222–223
global cybersecurity issues, 275–277
attribution problems, 281
Council of Europe, 284
foreign relations, 270
IETF, 192, 278–279, 280
Internet coordination, 277–279
lack of transnational authority, 281–282
NATO and, 283–284
United Nations efforts, 283
globalized supply chains, 166, 170
goals
CONOPS, 138
establishing, 118–119
failure to establish, 123
missions, 114
operational planning model, 124
reviewing plans against, 120–121
Gonzalez, Albert, 272
"good faith efforts," 217–218
"goodness of fit," 292
Google, 190, 198, 276
.gov domains, 192
Government Accountability Office. *See* GAO
GPS tracking devices, 269
Gramm-Leach-Bliley Financial Modernization Act (GLB), 222–223
grand juries, 273
graphical user interface (GUI), 182
Great Worm (Morris), 8–9, 270
green project status, 165
GSA (General Services Administration)
Brooks Act procurement, 77
functions of, 73
procurement role, 83
project management/acquisition phase, 143
responses to RFPs, 147–148
tensions over control, 78–80
GUI (graphical user interface), 182
guidance, defined, 304
guidance statements (DHS), 130–131
"Guide for the Security Certification and Accreditation of Federal Information Systems" (NIST SP 800-37), 172
guilty pleas, 274

H

H_a (alternative hypotheses), 39, 49, 291
hackers
attribution, 190, 195, 281
boy genius, 5–6, 27
Computer Fraud and Abuse Act, 270–272
criminal prosecution, 270–272
ethical hackers, 208
federal crimes, 269–270
federal prosecution process, 273–275
history of, 3–10, 275–276
identity theft, 219, 270, 271, 273
international issues, 281–282
monitoring for, 204
nation-state. *See* nation-state hackers
organized crime. *See* organized crime groups
personal information breaches, 219–222
prosecution of, 6, 9, 268–275
strength of, 57, 295, 296
in threat spectrum, 28
types of attacks, 187
Wiretap Act, 272
hard drives, 182, 185
hardware, 181
insecurity of, 202
IT systems, 185
physical security, 236
procurement. *See* acquisitions and procurement
securing, 220
harms. *See* damages
hashing, 194–195
Health and Human Services Department, 172, 225, 241
Health Information Technology for Economic and Clinical Health Act (HITECH), 225, 241
health insurance companies, 225
Health Insurance Portability and Accountability Act (HIPAA), 172–174, 223–225, 241
healthcare fraud, 217
healthcare provider security, 223–225
healthcare records, 172–174, 219–222, 223–225
Heartland Payment Systems, 272

high-level directives, 127, 128–131, 132–136
high-level requirements (HLRs), 132–137
higher courts, 268
higher-order languages, 181
HIPAA (Health Insurance Portability and Accountability Act), 172–174, 223–225, 241
HITECH (Health Information Technology for Economic and Clinical Health Act), 225, 241
HLRs (high-level requirements), 132–137
H_0 (null hypotheses), 39, 49, 290, 291
"holes," patching, 195
Homeland Security. *See* DHS
Homeland Security Act of 2002, 93–95, 129, 134, 261
Homeland Security Council, 91
Homeland Security Presidential Directives. *See* HSPDs
honeypots, 207, 237
"the hopper," 261
hops, 190
hosts, 185
House of Representatives, 261–263. *See also* Congress
HRA (human reliability analysis), 53
HSA (Homeland Security Act of 2002), 93–95, 129, 134, 261
HSPDs (Homeland Security Presidential Directives)
  Bush administration, 255
  HSPD-7 (Homeland Security Presidential Directive 7), 7, 95–97, 104, 129, 257
  HSPD-23 (Homeland Security Policy Directive 23), 99–102, 257
HTTP protocol, 194
HTTPS protocol, 194
"Human Capital" block, 125
human error, 41–46, 53, 200, 233
human reliability analysis (HRA), 53
human rights groups, 279
hypotheses
  creating, 248, 249
  cybersecurity research, 246
  designing, 39
  examples, 39
  null and alternative, 39, 49, 290, 291
  quantitative testing, 49

I

IANA (Internet Assigned Numbers Authority), 277
IBM personal computers, 4–5
ICANN (Internet Corporation for Assigned Names and Numbers), 192, 277–278, 279
ICT (information and communications technology), 166
ideal levels of risk, 36
identifying
  attackers (attribution), 190, 195, 281
  critical infrastructure, 95–97
  threats, 205–208
identity theft, 219, 270, 271, 273
Identity Theft Penalty Enhancement Act, 270, 273
IDS (intrusion detection system), 30
  corporate implementation, 237–238
  DHS monitoring case study, 162
  internal monitoring, 205
  role in cybersecurity operations, 204
  signatures and, 206
  vulnerabilities, 30
  warning systems, 111, 207
IETF (Internet Engineering Task Force), 192, 278–279, 280
IGCE (independent government cost estimate), 146–147
ignoring attacks, 207
IGs (inspectors general), 171
illegal wiretaps, 272
IMP (integrated master plan), 148, 149, 168
impact, 31
  identifying for projects, 123
  identifying in CONOPS, 140
  identifying in MNS, 136
"improbable" events, 15–16
IMS (integrated master schedule), 148, 149, 168
in-house monitoring, 204–205
"in motion" encryption, 194, 198
"in the wild" vulnerabilities, 201–202
incentives, 87, 103, 145
incorporation, 214
independent events (probability), 48–49
independent government cost estimate (IGCE), 146–147
independent variables (modeling), 56, 292, 293, 294
independent variables (research), 247
indicators (variables), 47, 53
indictments, 273
indirect consequences, 30
indirect relationships (logit models), 56
industrial espionage, 28. *See also* espionage
industries. *See* private sector
inferior courts, 268
information and communications technology (ICT), 166
information assurance, 72
information auditing, 240–241
information resources
  CIWG review, 86
  cybersecurity and, 70, 71
  data. *See* data

government's growth in, 81–82
internal and external, 119
researching. *See* research methods; research sources
information security, 97, 166, 170–172
information sharing, 89–90, 103, 223, 230
Information Sharing and Analysis Center (ISAC), 89–90, 230
information sharing policies, 223
Information Systems Audit and Control Association (ISACA), 240
information technology. *See* IT systems
information technology audits, 167
Information Technology Management Reform Act (Clinger-Cohen), 83–84, 126, 168–169
information warriors, 28
infrastructure. *See* critical infrastructure
initiating events (probability analysis), 50
Initiative #3 (CNCI), 99
insider threats, 200, 233
inspectors general (IGs), 171
insurance, 61–62, 238
integrated master plan (IMP), 148, 149, 168
integrated master schedule (IMS), 148, 149, 168
integrity of data, 187
intelligence agencies
CNCI directives, 99–102
FISMA requirements and, 98
ISAC participation, 90
military and civilian, 71–73
monitoring civilian networks, 100
intention (threat assessment), 25–26
"Inter-Intra-Agency Requirements" block, 124
intercepting communications, 272
interdependencies (IMS), 148
interim final rules, 267
internal audits, 166–168, 239–241, 240
internal constraints, 123
"Internal Control-Integrated Framework," 239
internal controls, 230, 239–241
internal information gathering, 162
internal monitoring, 204–205
internal project information, 119
internal risks, 240
internal systems (corporate), 218
internal threats, 28
international issues. *See* global cybersecurity issues
International Strategy for Cyberspace, 259
Internet
attacks and exploits, 195–202
BGP connections, 190–192
dependency, 275
diagrammed, 186
DNS system, 192
encryption methods, 193–195
global management of, 275
growth of, 186–187
history of, 179, 185–187
IANA/ICANN/IETF, 277–280
insecurity of, 202
operations of, 188–189
origins of, 4
protocols, 189–190
structure of, 187–188
Internet Assigned Numbers Authority (IANA), 277
Internet Corporation for Assigned Names and Numbers (ICANN), 192, 277–278, 279
Internet Engineering Task Force (IETF), 192, 278–279, 280
Internet Protocol. *See* IPv4; IPv6; TCP/IP
Internet Protocol Security (IPSec), 279
Internet service providers (ISPs), 188, 202, 204
interstate commerce crimes, 271
interviews, 40, 288
"An Introductory Resource Guide for Implementing the HIPAA Security Rule" (NIST 800-66), 174
intrusion detection systems. *See* IDS (intrusion detection system)
intrusion prevention systems. *See* IPS (intrusion prevention system)
investment
duty of care, 215–219
justifying, 133, 135–136
SEC disclosures and, 229
investment advisors, 228
IP addresses, 189–190
BGP functions, 190–192
DDoS attacks, 198
DNS and, 192, 278
DNS cache poisoning, 200
faking, 191–192
global Internet management, 277–279
human-readable, 192
translating, 188
vulnerabilities, 190
IP (Internet Protocol)(TCP/IP), 187, 188, 189
IP (Office of Infrastructure Protection), 94, 131
IPS (intrusion prevention system)
cybersecurity operations role, 204
Einstein 3, 99–100
internal monitoring, 205
signatures and, 206

as warning system, 207
IPSec (Internet Protocol Security), 279
IPv4 (Internet Protocol version 4), 189, 279
IPv6 (Internet Protocol version 6), 189, 279
Iran
offensive cyber capabilities, 37
DDoS attacks, 10, 198
drones, 276
Flame virus, 102, 276
Stuxnet virus, 10, 102, 275–276
ISAC (Information Sharing and Analysis Center), 89–90, 230
ISACA (Information Systems Audit and Control Association), 240
ISPs (Internet service providers), 188, 202, 204
Israel, 10, 37, 102, 276
"IT Capital Asset Summary," 170
IT systems, 18
audits, 167, 173
best practices, 126
Clinger-Cohen Act, 126
communication pathways, 185
corporate assessments, 233
corporate governance and, 216
costs, 160
Exhibit 300 reports, 169–170
hardware in, 185
health care providers, 224
internal controls, 239–240
procurement, 83
repairing, 237
software in, 185
Sony PlayStation breach, 221
standards for, 169
systems in, 185
vulnerabilities, 30

J
Java, 181
judicial branch of government, 268–270
CFAA rulings, 270–272
cybersecurity role, 250–251, 269–270
federal criminal process, 273–275
federal regulations and, 267–268
identity theft rulings, 273
Justice Department, 72, 90
structure of, 268–269
Wiretap Act rulings, 272
judicial precedent, 269
jurisdiction, 269–270, 281–282
Justice Department, 72, 90
justification section (MNS), 134, 135–136

K
Kennedy administration, 95
keyboards, 181
keys (encryption), 193, 271
kiddy hackers, 5–6, 27
known exploit signatures, 206
known vulnerabilities, 201
Kosovo, 276

L
L-3 security breach, 213
labor, 109, 125, 146
LACNIC (Latin America and Caribbean Network Information Centre), 279
LANs (local area networks), 188
laptops, 182, 183
Latin America and Caribbean Network Information Centre (LACNIC), 279
law enforcement agencies, 89–90, 202, 236–237, 281
laws, 69. *See also* legislation
lawsuits, 216–219, 220, 221–222
leading questions (surveys), 288
legal system. *See* judicial branch of government
legislation, 304. *See also* specific acts of law (Brooks Act, Computer Security Act, etc.)
CIWG review, 86
compliance, 167
congressional process, 261–263
Congress's mandates, 251, 260
crafting, 74
cybersecurity and, 69–70, 261
federal regulations and, 265–268
government agencies/branches, 70–74
history of cyber law
origins (1945-1984), 74–77
control conflict (1984-1995), 77–81
cyber developments (1995-2001), 81–90
Homeland Security (2001-2008), 90–98
CNCI/cyber warfare (2008-present), 99–102
recent developments, 102–104
impact on projects, 123
law, defined, 69
mission requirements and, 127, 128
passing bills into law, 261–263
private sector regulations, 222–230
protecting personal information, 212
state laws, 227–228
legislative branch of government. *See* Congress
lethality, 25, 26–27

leveraging technologies, 159
liabilities
  data breaches, 219–222
  duty of care, 217–218
Library of Congress, 264–265
Lieberman, Joseph, 102–103
lifetimes (programs), 133, 135, 136
likelihood, 37, 38, 59. *See also* probability
line functions, 116
linear regression models, 292
local area networks (LANs), 188
local threats, 233
Lockheed Martin, 213
logging attacks, 207
logic decision processes, 55
logical fallacies, 249
logistic regression equation for probabilities, 294, 295
logistic regression (logit), 56–57
logit models, 56–57, 292–293
logs, 236
Los Alamos National Laboratory, 6
lower-order programming languages, 180–181
Lulz Security (LulzSec), 19

M
M memoranda. *See* OMB
machine code, 180–181
magnetic badges, 236
magnitude of risk, 37, 47
mainframe computers, 75–76, 185
malware, 195, 196, 271
man in the middle attacks, 198–199
"manage" task (risk management), 15
management and acquisition phase (Op Model), 143–148
"Management of Information Resources," 83
managers, 113. *See also* program/project managers; senior managers
  compliance and reporting, 166–174
  constraints, 123–124
  coordinating functions, 115–117
  corporations, 214–215
  cybersecurity framework. *See* cybersecurity management framework
  in cybersecurity operations, 202
  cyclical nature of management, 121
  decision-making processes, 117–121
  earned value management, 148–165
  functions of, 109–110
  goals/missions and, 114–115
  management and acquisition, 143–148
  managing *vs.* doing, 113–114
  measurable outcomes, 117
  operational planning model, 124–125
  strategies and plans, 114–115
  types of, 109–110
  US-CERT failure case study, 122–125
managing risks. *See* risk management
"marginal" label (GAO), 31–33
Marine Corps, 71
Marine Corps Intelligence, 72
mark-up sessions, 262
material costs, 146
"material information" disclosures, 229
mathematical risks, 53–55
MB (megahertz), 182
McAfee Inc., 114, 115
McVeigh, Timothy, 85
MD5 (message digest hash), 194–195
"Measurement" block, 125
measurements. *See* metrics and measurements
medical records, 172–174, 219–225. *See also* HIPAA
Medicare and Medicaid fraud, 217
megahertz (MB), 182
memory, 182, 184–185
message digest hash (MD5), 194–195
metrics and measurements
  DHS monitoring case study, 163
  establishing, 118–119, 123
  EVM accounting, 148
  EVM measurements, 151–154
  failure to establish, 123
  FISMA requirements, 171
  identifying in MNS, 135
  metrics, defined, 117
  op models, 140–142
  operational planning models, 125
  plan outcomes, 117
  in PWSs, 145
  qualitative research, 40
  red, yellow, and green status, 165
  reviewing plans against, 120–121
  risk research questions, 39
  WBS tasks, 150
microphone activation, 102
Middle East, 279
milestones
  DHS monitoring case study, 160
  identifying, 135
  IMS depiction, 148
  operational requirements documents, 140
  POA&M documents, 147–148
military. *See also* Defense Department
  agencies and commands, 71–73

CNCI directives, 99
FISMA requirements and, 98
role in cybersecurity, 69–71
tensions over control, 70, 71, 78–81, 104–105
minicomputers, 185
minimum operational values, 142
misconfiguration, 201
mission needs statement. *See* MNS
missions, 109
driving projects, 123
operational planning model, 124–125
strategies and plans, 114, 115
mistakes of logic, 249
mitigating damages, 237
mitigating risks
federal CIOs role, 84
as high-level requirement, 136
risk levels and, 36
in risk management framework, 16, 20
risk responses, 60, 61
Mitnick, Kevin, 5–6
MNS (mission needs statement)
authorization section, 134–135
capabilities in, 133–134
capability gaps, 133–134
courses of action, 135
developing, 126–127
high-level input sources, 131, 132–136
high-level requirements, 132–137
justification section, 134, 135–136
lifetimes, 135
outcomes, 135
translating into capabilities, 132–133
model corporate cybersecurity program, 231
board of directors, 231–232
business continuity plans, 238
CEO and CIO roles, 232
education and training, 235
encryption, 235–236
intrusion detection systems, 237–238
penetration testing, 234–235
physical security, 236
response program, 236–237
risk assessment, 232–234
vendor management, 238
written plans, 234
monitoring internal controls, 241
monitoring risks
Citigroup lawsuit, 218–219
compliance, 62–63, 64
corporate implementation, 237–238
corporate responsibilities, 218
cybersecurity operations, 203–205
DHS case study, 158–164
effectiveness, 62–63, 64
as high-level requirement, 136
identifying changes in environment, 62–63, 64
internal monitoring, 204–205
obligations, 221–222
policy monitoring, 205–206
risk management framework, 16, 17, 18, 20
tool list, 205
Monte Carlo analysis, 53–55
Morris, Robert Tappan, 8–9, 270
Morris worm, 8–9, 270
mortgage crisis, 218–219
motherboards, 181, 182
multi-core processors, 182
multiple-choice questions, 288–289, 290
multiple processors, 182
multivariate statistical analysis, 53–55, 58–60
mutually-exclusive events (probability), 48–49

N

NASA (National Aeronautics and Space Administration), 47
Natanz nuclear facility, 10
nation-state hackers
early cyber spying, 6
international cyber defense capabilities, 37
international law enforcement, 281–282
levels of risk and, 35
monitoring for, 204
threat assessments, 27
National Aeronautics and Space Administration (NASA), 47
National Bureau of Standards. *See* NIST
National Communications System, 94, 95
national coordinator for security, infrastructure protection and counter-terrorism, 88
National Cyber Security Center, 130
National Cyber Security Division (NCSD), 122
National Cybersecurity and Communications Integration Center (NCCIC), 94, 122
National Cybersecurity Council, 103
National Geospatial Intelligence Agency, 72
National Infrastructure Advisory Council, 93
National Infrastructure Assurance Council, 87
National Infrastructure Protection Council (NIPC), 89–90, 94–95, 261
National Infrastructure Protection Plan (NIPP), 18, 87, 94, 96, 97, 104
National Institute for Standards and Technology. *See* NIST

national intelligence workers, 28
National Nuclear Security Agency (NNSA), 41–46
National Policy for Infrastructure Protection, 87
National Policy on Telecommunications and Automated Information Systems Security (NSDD-145), 7–8, 78–80
National Protection and Programs Directorate (NPPD), 94, 122, 131
National Reconnaissance Office, 72
National Science Foundation, 4
National Science Foundation Network (NSFNET), 4
national security
  board of directors role in, 231–232
  civilian *vs.* military cybersecurity control, 70, 71
  criminal information access, 270
  personal computers and, 5
  procurement function and, 77
  sentencing and, 275
  threat spectrum, 28
National Security Act, 253
National Security Agency. *See* NSA
National Security Council (NSC), 74, 87, 93, 253
National Security Decision Directives (NSDDs), 7–8, 78–80
national security instruments, 74, 255
  as authorization, 134
National Security Policy Directives. *See* NSPDs
"National Strategy to Secure Cyberspace," 95
National Vulnerability Database (NVD), 201
NATO Computer Incident Response Capability (NCIRC), 283–284
NATO (North Atlantic Treaty Organization), 101, 276, 283–284
Navy
  attacks on, 276
  Office of Naval Intelligence, 71, 72
NCCIC (National Cybersecurity and Communications Integration Center), 94, 122
NCIRC (NATO Computer Incident Response Capability), 283–284
NCSD (National Cyber Security Division), 122
negative relationships (logit models), 56
"negligible" label (GAO), 31–33
NERC (North American Electric Reliability Corporation), 229–230
NERC Standard CIP-008-4, 230
Netherlands' cyber defenses, 37
network cards, 182
networks
  altering configuration during attacks, 207, 237
  anomalies, 162–163, 203, 206–207, 237–238
  BGP connections, 190–192
  civilian network monitoring, 100
  CNCI protections, 99–102
  continuous monitoring systems, 122–123
  cybersecurity operation capabilities, 202–208
  denial of service attacks, 198, 203, 204, 275
  early policy decisions, 7–8
  firewalls. *See* firewalls
  FISMA protection, 97
  honeypots, 207, 237
  ISP access to, 188
  liability for data breaches, 219–222
  monitoring case study, 158–164
  types of, 188
  vulnerabilities, 200–202
  zombie networks, 198
Network Security Deployment division (NSD), 94
New Deal agencies, 75
New York state law, 216
New Zealand, 279
Nichols, Terry, 85
NIPC (National Infrastructure Protection Center), 89–90, 94–95, 261
NIPP (National Infrastructure Protection Plan), 94, 96
  Clinton administration commissions, 87
  DHS goals in, 97
  DHS risk management, 18
  Office of Infrastructure Protection, 94, 131
  replacing, 104
NIST (National Institute for Standards and Technology)
  compliance, 171
  functions of, 73
  "Guide for the Security Certification and Accreditation of Federal Information Systems," 171–172
  IT vulnerabilities list, 30
  NIST 800-53 (Recommended Security Controls for Federal Information Systems and Organizations), 174
  NIST 800-66 (An Introductory Resource Guide for Implementing the HIPAA Security Rule), 174
  NVD (National Vulnerability Database), 201
  "Recommended Security Controls for Federal Information Systems and Organizations," 174
  risk management frameworks, 18, 98
  security practices role, 80
Nixon administration, 253–254
NNSA (National Nuclear Security Agency), 41–46
non-experimental research, 247–248
non-volatile memory, 184, 185
noncompliance consequences, 172
North American Electric Reliability Corporation (NERC),

229–230
North Atlantic Treaty Organization (NATO), 101, 276, 283–284
Northeast Blackout, 2003, 92
Norway, 4
"Not Applicable" answers, 288
not-mutually exclusive events (probability), 48–49
notice and comment period, 266–267
notifications. *See also* alerts; warning systems
as capability, 203
costs of, 236
as passive response, 207
state laws, 227–228
NPPD (National Protection and Programs Directorate), 94, 122, 131
NRC (US Nuclear Regulatory Commission), 47, 53
NSA (National Security Agency)
civilian/military control tensions, 78–81
classified computer systems and, 80
Einstein 3 program, 99–100
founding of, 128
role in cybersecurity, 71–73
NSC (National Security Council), 74, 87, 93, 253
NSD (Network Security Deployment division), 94
NSDD-145 (National Policy on Telecommunications and Automated Information Systems Security), 7–8, 78–80
NSFNET (National Science Foundation Network), 4
NSPDs (National Security Policy Directives)
Bush administration, 255
CNCI, 99–102
NSPD-54 (National Security Policy Directive), 99–102, 130, 257
nuclear arms, 6, 7
nuclear facilities
criminal information access, 270
human reliability in management, 53
PRA risk management, 47
virus attacks, 102, 276
Nuclear Regulatory Commission (USNRC), 47, 53
null hypotheses (H_0), 39, 49, 290, 291
NVD (National Vulnerability Database), 201
NY BCL (Business Corporation Law of New York State), 216

O

Obama administration
cybersecurity initiatives and policies, 98–104
Cyberspace Policy Review, 130
executive orders, 104, 256
national security instruments, 104, 255
objective values (management), 142–143
objectives, 138, 146
OCIA (Office of Cyber and Infrastructure Analysis), 94, 131
ODNI (Office of the Director of National Intelligence), 72
off-site back-ups, 236
OEC (Office of Emergency Communications), 94
Office of Cyber and Infrastructure Analysis (OCIA), 94, 131
Office of Cybersecurity and Communications (CS&C), 94, 122, 131
Office of E-Government and Information Technology, 254
Office of Emergency Communications (OEC), 94
Office of Homeland Security. *See* DHS
Office of Information and Regulatory Affairs, 82, 254
Office of Infrastructure Protection (IP), 94, 131
Office of Management and Budget. *See* OMB
Office of National Infrastructure Assurance, 87
Office of Science and Technology Policy (OSTP), 254, 259
Office of the Director of National Intelligence (ODNI), 72
Office of the National Counterintelligence Executive (ONCIX), 72
OHS (Office of Homeland Security). *See* DHS
OIRA (Office of Information and Regulatory Affairs), 82, 254
Oklahoma City bomb, 85–86, 256
Olympic Games cyberwar program, 102
OMB (Office of Management and Budget)
circulars
A-11 (capital assets), 149, 150
A-130 (information resource management), 83, 172
Exhibit 300 reports, 169–170
FISMA compliance, 98, 171
FISMA oversight, 102–103, 129
functions of, 73
information management, 82–84
IT system requirements, 169–170
memoranda, 258–259
M-08-05 (trusted Internet connections), 138–139
M-10-28 (DHS responsibilities), 103, 257, 258–259
M-97-02 (funding information systems), 83
role of, 253–254
TIC mandate, 22, 138–139, 258
ONCIX (Office of the National Counterintelligence Executive), 72
online retailer examples, 55–60, 292–296

online surveys, 289–290
ontology, 246–247
op models (operating models), 142, 143–148, 160
open-ended questions, 288, 290
open standards organizations, 279
operating models (op models), 142, 143–148, 160
Operation Aurora, 276
operational planning models, 124–125
operational processes (CONOPS), 138
operational requirements document (ORD), 140
opting out (financial information), 223
oral communications, 272
ORD (operational requirements document), 140
"Organizational Capital" block, 124–125
organizational structure, 123
organizations, 109
  impacts of structures, 123
  top-down analysis, 50–52
organized crime groups, 19
  levels of risk and, 35
  prosecution, 268–275
  risk determination example, 36
  risk management outline, 20
  threat assessment, 25, 26–27
  in threat spectrum, 28
OSTP (Office of Science and Technology Policy), 254, 259
OSTP Resource Library, 254
"Other" answers, 288
outcomes
  in CONOPS, 140
  defining, 135
  measurable, 117
  in op models, 140–142
  operational planning model, 124
  in PWSs, 145
  regression modeling, 56
  success and, 120
over budget status, 156, 163
overriding vetoes, 263
oversight
  congressional, 74
  corporate failure, 215–219
  duty of care, 217

P

p-values, 291
Pacific Bell, 5
packet analyzers (sniffers), 204, 272
packets, 187, 188–189
Paperwork Reduction Act (PRA), 82, 254
participants in CONOPS, 138
passive responses to threats, 207–208, 237–238
passwords
  brute force attacks, 193
  corporate data, 220
  corporate policies, 235
  corporate systems, 233
  logit analysis, 295, 296
  selling, 271
  strong passwords, 57, 220, 235
  as vulnerabilities, 200
  wireless systems, 227
patches, 195, 200, 227
Patriotic Hacker attacks, 276
Payment Card Industry Data Security Standards, 221
PCCIP (President's Commission on Critical Infrastructure Protection), 86–87, 255, 257
PCs (personal computers)
  attacks and exploits, 195–202
  changes in national security and, 77–81
  criminal information access, 271
  cybersecurity operation capabilities, 202–208
  early federal policies, 7–8
  early years of, 4–5
  FISMA protection, 97
  in IT infrastructure, 185
  protected computers, 272
  systems, 182–184
  virus attacks, 102
  vulnerabilities, 200–202
  worms, 8–9
PDDs (Presidential Decision Directives), 74. *See also* national security instrument
  Clinton administration, 74, 255
  PDD-63
    critical infrastructure protection, 87–90
    energy information sharing, 230
    HSA elements of, 261
    Oklahoma City response, 255
    replacement of, 257
penetration testing, 234–235
percentages (comparing projects), 157–158
performance
  APBs, 142
  objective and threshold values, 142–143
  red, yellow, and green status, 165
performance-based acquisitions, 145–146
"performance measurement report," 170
performance work statements (PWS), 144, 145–146
period of performance (POP), 155, 164
personal computers. *See* PCs
personal information
  bank sales of, 222

business's duty towards, 212–213
civilian *vs.* military cybersecurity control, 70, 71
criminal computer access, 271
criminal information access, 273
customer information leak example, 55–60
liability for breaches, 219–222
phishing attacks, 197–198
protected health information, 173
Sony PlayStation Network breach, 221–222
spear phishing attacks, 41–46
TJX data breach, 220, 226–227, 272
personal interviews, 40, 288
PHI (protected health information), 173, 225
phishing attacks, 41–46, 197–198
phone companies, 188
phone surveys, 40
physical security, 236
plan of action and milestones (POA&M), 147–148
planned value. *See* PV (planned value)
planning, programming, budgeting and execution (PPBE), 127
plans, 114–115
alternative scenarios, 119–120
assessing, 120
capability-based planning, 136–137
choosing, 120
CONOPS, 137–140
executing, 120
measurable outcomes, 117
op models, 140–142
operational planning model, 124–125
POA&M documents, 147–148
plausible deniability, 281
plea bargains, 274
POA&M (plan of action and milestones), 147–148
Poindexter, John, 7–8, 78–81, 98
point system (sentencing), 274–275
policies
as authorization, 134
compliance, 167
in CONOPS, 138, 140
federal. *See* policies (federal)
impact on projects, 123
internal controls, 239–240
mission needs statements and, 128–130
policy directives, 304
policy monitoring, 205–206
policies (federal), 69
agencies involved in, 70–74
crafting, 74
cybersecurity and, 69–70
Cyberspace Policy Review, 100–101
DHS frameworks, 95
FISMA requirements, 98
history of cybersecurity, 70–74
origins (1945-1984), 7–9, 74–81
control conflict (1984-1995), 77–81
cyber development (1995-2001), 81–90
Homeland Security (2001-2008), 90–98
CNCI/cyber warfare (2008-present), 99–102
recent developments, 102–104
sentencing, 274
policy directives, 304
policy monitoring, 205–206
POP (period of performance), 155, 164
population, 41, 289–290
positive relationships (logit models), 56
power grid. *See* electrical grid
power plants, 229–230
PPBE (planning, programming, budgeting and execution), 127
PPDs (Presidential Policy Directives), 255
PRA (Paperwork Reduction Act), 82, 254
PRA (probabilistic risk assessment)
event tree analysis, 49–52
fault tree analysis, 50–52, 53, 54
human reliability analysis, 53
logistic regression equation, 294, 295
Monte Carlo analysis, 53–55
quantitative risk determination, 47–48
precedents, judicial, 269
predicting leaks, 58–60
predicting threats, 206–207
predictive analysis, 206–207
preponderance of evidence, 281
presidential directives, 74, 129. *See also* executive orders; national security instruments; HSPDs
mission requirements and, 127, 128–130
Presidential Policy Directives (PPDs), 255
PPD-21, 104
Presidential Study Directives (PSDs), 255
presidents
agency creation, 266
agency supervision, 74
bill signing or vetoing, 263
cybersecurity policy role, 69–70
Executive Office of. *See* EOP
executive orders. *See* EOs
as first responders, 251, 252
military or civilian security control policies, 71
mission requirements, 127, 128–131
national security instruments, 74
presidential directives, 74, 129. *See also* executive orders; national security instruments; HSPDs

scope of power, 128–130
as senior managers, 110
President's Commission on Critical Infrastructure Protection (PCCIP), 86–87, 255, 256
President's Council on Year 2000 Conversion, 89
primary consequences, defined, 30
printers, 182, 183
priorities
FISMA requirements, 171
risk management framework, 16, 20, 21, 23
privacy issues
bank sales of personal information, 223
civilian *vs.* military cybersecurity control, 70, 71
court cases, 269
IPv6 and, 279
policy formation, 74
Privacy Rule (HIPAA), 224
private corporation governance, 213–215
private-public partnerships
board of directors role, 231–232
critical infrastructure protection, 70, 85, 87–88, 105
DHS agencies charged with, 94, 96
DHS strategies, 259
incentives for, 87, 103, 145
National Infrastructure Assurance Council, 87
outlining shared threats, 87, 99
policy formation, 74
post 9/11, 92–93
threats to critical infrastructure, 87
private sector
business interruption insurance, 238
corporate governance, 213–222
critical infrastructure owned by, 85
cyber incident reports, 103
cybersecurity overview, 211–213
duty of care, 213–222
electrical grid, 229–230
HIPAA compliance, 172–174
incentives for partnerships, 87, 103, 145
internal audits and controls, 239–241
legislative requirements, 222–230
liabilities, 213–222
model cybersecurity programs, 231–238
NSDD-145 computer security issues, 8
partnerships. *See* private-public partnerships
policy formation, 74
protecting critical infrastructure, 70, 85–88, 105
risk management strategies, 212
Sarbanes-Oxley Act and, 230
SEC disclosures, 228
security roles, 231–232
strategy questions, 211–213
proactive safeguards, 220, 231
probabilistic risk assessment. *See* PRA (probabilistic risk assessment)
probability
calculating, 35–37
illustrated, 38
logistic regression equation, 295–296
PRA risk management, 47. *See also* PRA
predicting leaks with statistical analysis, 58–60
probability distribution, 48
probability sampling, 290
probability theory, 48–49
quantitative risk determination, 48–49
values, 54
probable cause, 273
procedures, 114, 167
processors, 181–182
procurement. *See* acquisitions and procurement
"Products and Services" block, 124
professional auditors, 241
program/project managers, 110, 113
comparing projects, 157–158
compliance and reporting, 166–174
CONOPS, 137–140
defining capabilities, 136
DHS cybersecurity programs, 127
earned value management, 148–165, 298–302
forecasting, 300–302
function coordination, 115–116
high-level requirement analysis, 132
management and acquisition, 143–148
mission needs statements, 126–127
objective and threshold values, 142–143
op models, 140–142
tracking projects, 153–157
warning system example, 110–113
programming languages, 180–181
programs. *See* software
project managers. *See* program/project managers
proposed bills, 261–264
proposed rules, 260, 266
prosecution of cybercriminals, 6, 9, 268–275
prosecutors, 273
protected computers, 272
protected health information (PHI), 173, 224
protection
as capability, 203
as high-level requirement, 136
infrastructure. *See* critical infrastructure protection

networks, 97, 99–102
PCs, 97
personal information, 173
protected computers, 272
protective markings, 79
protocol identifier assignments, 277
protocols, 188, 189–190, 277
PSDs (Presidential Study Directives), 255
public corporation governance, 213–215
public hearings, 260, 262, 266
public image, 212
public-private partnerships. *See* private-public partnerships
PV (planned value)
District Design case study, 152–154
percentages, 157–158
schedule variances, 154–155
SPI equations, 299
PWS (performance work statement), 144, 145–146

Q

Quadrennial Homeland Security Review report to Congress (QHSR), 130, 259
qualitative risk determination, 37–46
quantitative risk determination, 37–39, 47
event tree analysis, 49–52
fault tree analysis, 50–52, 53, 54
human reliability analysis, 53
Monte Carlo analysis, 53–55
online retailer example, 55–60
probabilistic risk assessment, 47–48
probability basics, 48–49
statistical modeling, 55
questionnaires. *See* survey designs
questions
advanced research methods/sources, 284–286
computer technical fundamentals review, 208
cybersecurity law and policy review, 105–107
cybersecurity management review, 174–176
private sector cybersecurity review, 242–243
qualitative research questions, 39–41
research questions, 247
risk determination review, 65–66
risk research questions, 38–39

R

radio signal badges, 236
RAM (random access memory), 182, 184–185
random sampling, 290
ratings agencies, 228
re-engineering backwards, 141
Reagan administration, 7–8, 74, 78–80, 128
reason, mistakes of, 249
reasonable doubt, 274
reckless behavior, 271
"Recommended Security Controls for Federal Information Systems and Organizations" (NIST SP 800-53), 174
reconciliation, 263
reconnaissance attacks, 196
recovery from attacks
business continuity plans, 238
as capability, 203
corporate policies, 237
"National Strategy to Secure Cyberspace," 95
red project status, 165
reducing risk (capability), 159
regional Courts of Appeals, 268
Regional Internet Registries (RIRs), 278–279
registries (Internet addresses), 278–279
regression modeling, 56, 291, 292, 294–295
regulations, 265–266, 304
Code of Federal Regulations, 268
compliance, 167
Congressional and Judicial roles in, 267–268
creating, 266–267
Federal Register publication, 260
impact on projects, 123
regulatory agencies, 236–237
reliability, 39
reliability standards (NERC), 230
reliability tests, 249
Reno, Janet, 86
rental botnets, 198
repairing systems, 237
reports
audits, 166–168
corporate policies, 235, 237
DHS cybersecurity reports, 130–131
energy grid cybersecurity, 230
Exhibit 300, 169–170
federal government practices, 168–169
FISMA requirements, 170–172
health care system breaches, 225
internal controls, 239–240
operational planning model, 125
Sarbanes-Oxley Act, 230
Requests for Comments (RFCs), 279
requests for information (RFIs), 143–144
requests for proposals (RFPs), 144–148
research methods, 245–249
research questions

creating, 247
dependency on Internet, 275
risk research, 38–39
spear phishing attack vulnerabilities, 41–46
statistical modeling, 56
survey design, 288–296
research sources
Code of Federal Regulations (CFR), 268
Council of Europe, 284
executive branch, 251–260, 254
executive orders, 256–258
Federal Register, 260
OMB memoranda, 258–259
OSTP memoranda, 259
national security instruments, 255
White House strategy and guidance, 259
GAO website, 264
government documents, 249–251
Internet Engineering Task Force, 279
legislative, 264–265
Congressional Record, 264
Congressional Research Service, 264–265
proposed bills and law, 264
NATO, 283–284
THOMAS.gov, 264
United Nations, 283
research subjects, 248
Réseaux IP Européens Network Coordination Centre (RIPE NCC), 279
resources
as constraints, 21
decision-making process, 121
identifying in MNS, 135
impact on projects, 123
management and acquisition phase, 143–148
POA&M documents, 147–148
risk monitoring and, 63
time and money, 150–152
trade-offs in risk management, 23
responding to attacks
active responses, 207–208, 237–238
containing threats, 61
corporate plans, 234, 236–237
NATO teams, 284
passive responses, 207–208, 237–238
presidents as first responders, 251, 252
types of responses, 207–208
responding to risks
acceptance, 16, 20, 36, 60–61
avoidance, 60, 61
as capability, 203
cybersecurity insurance, 61–62
as high-level requirement, 136
mitigation, 60, 61
risk management framework, 16, 17, 18, 20
risk responses, defined, 60
transfer, 16, 20, 60, 61–62
unacceptable risks, 22
response rates (surveys), 42
responsibilities in CONOPS, 138, 140
restitution to victims, 273
results, assessing, 120–121
reviewing warnings, 112
RFCs (Requests for Comments), 279
RFIs (requests for information), 143–144
RFPs (requests for proposals), 144–148
Ridge, Tom, 90
RIPE NCC (Réseaux IP Européens Network Coordination Centre), 279
RIRs (Regional Internet Registries), 278–279
risk, 17
assessing. *See* risk assessments
benefits of, 64
determination. *See* risk determination
framing. *See* framing risks
graphing, 33
internal audits, 167
levels of, 33–37
management. *See* risk management; risk management frameworks
responding to. *See* responding to risks
risk equation, 23
risk formula, 23–33
severity, 37, 47
tolerances, 16, 20, 21, 22
unacceptable, 22
risk assessments, 23–24
audits, 240
Cybersecurity Act, 103
DHS monitoring case study, 161–162, 164
FISMA requirements, 97–98
model corporate cyber program, 232–234
risk determination and. *See* risk determination
risk equation, 23–24, 34–35
risk management framework, 16, 17, 18, 20
risk-based decisions, 19, 98
risk determination, 33–37
methodologies, 37–39
quadrant diagram, 36
qualitative methods, 37–46
quantitative methods, 37–39, 47–60
review questions, 65–66

risk assessment in, 33
risk equation, 23–25, 34–35
risk framing. *See* framing risks
risk management, 15–17
consequence assessment, 30–33
federal agency roles in, 83–84
frameworks, 16, 18
health care systems, 224
operational planning model, 125
organized crime example, 20
plans, 15
presidential directives for, 96
private sector strategies, 212
process, 18–19
risk, defined, 17
risk assessment, 23–33
risk determination, 33–60
risk formula, 23–33
risk framing, 19–23
risk managers, 26
SEC guidelines, 228–229
strategies, not checklists, 66
threat assessment, 25–28
threat shifting, 28
vulnerability assessment, 29–30
risk management frameworks, 16, 17, 18, 20
risk management plans, 15
risk research questions, 38–39
risk responses. *See* responding to risks
risk tolerances, 16, 20, 21, 22
roles (CONOPS), 138, 140
Roosevelt administration, 75, 128
root server management, 277
routers, 182, 183, 185, 187, 188, 190–192, 198–199
routing attacks through other countries, 282
routing tables, 190
RSA SecurID breach, 198, 212–213
rules, 205–206, 266
Russian-Chechen conflict, 276
Russian Federation, 279
Russian-Georgian conflict, 277

S

Safeguards Rule, 223
sample populations, 41, 289–290
Sarbanes-Oxley Act (SOX), 168, 230
satellites, 3
SBU IT (sensitive-but-unclassified information technology), 81
Scalia, Antonin, 269
scanning systems, 201, 205
Schedule Performance Index (SPI), 157, 298–299
schedule variances (SVs), 154–158, 163–164
schedules
acquisition performance baselines, 142
delays in, 163–164
DHS monitoring case study, 160
Integrated Master Schedules, 148, 149
manager's role, 117
objective and threshold values, 142–143
variances, 154–155
Schmidt, Howard A., 101
"Scientific Integrity," 259
scientific issues, 259
scientific methods, 248
screen locks, 235
search warrants, 272
SEC (Securities and Exchange Commission), 228–229, 237
SECIR (Stakeholder Engagement and Cyber Infrastructure Resilience division), 94
Secret Service, 90, 93
sector-specific agencies (SSAs), 96
sectors in management framework, 127
secure hash algorithm (SHA-2), 194–195
SecurID data breach, 198, 212–213
Securities and Exchange Commission (SEC), 228–229, 237
security
vs. accessibility, 22
certification and accreditation, 171–172
OMB role in, 82
security even correlation tools, 205
Security Rule (HIPAA), 224
self-administered surveys, 40, 41–46, 288
Senate, 261–263
senior managers, 110, 113, 115, 116
sensitive but unclassified information, 8, 78, 79, 233
sensitive-but-unclassified information technology (SBU IT), 81
sensitive information, 233
sentencing
CFAA offenses, 270–272
cyber criminals, 269
guidelines, 274–275
September 11, 2001
executive orders after, 257
reorganizations after, 90
risk planning after, 15–16
scope of presidential power and, 129
sequences of events, 50
servers, 185, 204, 220

service providers (ISPs), 188, 202, 204
severity of attacks, 207
severity of risk, 37, 47
SHA-2 (secure hash algorithm), 194–195
shared threats, 28, 87, 88
shareholders, 213, 214, 215–219, 221–222
shunning attacks, 207
signal intelligence, 72
signature-based tools, 99–100, 205, 206, 237–238
signatures
  digital, for DNS, 192
  IDS/IPS tools, 206
  internal monitoring, 205
  known exploits, 206
  threat signature technology, 99–100, 237–238
simulating attacks, 206–207, 234–235
SME (subject matter expert), 161
sniffers (packet analyzers), 204, 272
social engineering attacks, 235
social media phishing attacks, 197
Social Security numbers, 273
software, 182
  antivirus. *See* antivirus software
  exploits, 195
  IDS/IPS tools, 206
  insecurity of, 202
  in IT systems, 185
  malware, 195, 196, 271
  programs, defined, 181
  signature-based tools, 99–100, 205, 206, 237–238
  vulnerabilities, 200–202
Sony PlayStation Network, 221–222
SOOs (statements of objectives), 144, 146
South Ossetia, 277
sovereignty, 282
Soviet Union. *See also* Russian Federation
  Cold War, 3, 76, 78
  computer security and, 78
  Sputnik, 3
SOWs (statements of work), 144
SOX (Sarbanes-Oxley Act), 168, 230
SP 800-37 (Guide for the Security Certification and Accreditation of Federal Information Systems), 171
space allocation (ICANN), 277
Space Race, 3
spam filters, 197
Speaker of the House, 262
spear phishing attacks, 41–46, 197–198
Special Advisor for Cyberspace Security, 93, 257, 259
speed of processors, 182
SPI (Schedule Performance Index), 157, 298–299
spies. *See* espionage
sponsors, bills, 261
spoofed websites, 198
Sputnik, 3
SSAs (sector-specific agencies), 96, 104
staff functions, 116
staffing in models, 125
Stakeholder Engagement and Cyber Infrastructure Resilience division (SECIR), 94
stakeholders, 138, 140, 160
standard deviations, 291
standards, 304
state attorneys general, 220
state court jurisdictions, 269–270
State Department, 72
state laws, 227–228
statements of objectives (SOOs), 144, 146
statements of work (SOWs), 144
statistical modeling, 290–292
  Monte Carlo analysis, 53–55
  online retailer probability example, 55–60
  predicting leaks, 58–60
  quantitative risk determination, 55
  regression modeling, 56
"statistically significant," 290, 291
statutes, 304. *See also* legislation
steps (op models), 141
stock, 213–214, 228–229, 238
stock values, 212
storage, 184–185
strategic objectives in models, 124
"Strategic Risk Management" block, 125
strategies, 114, 115
  alternative scenarios, 119–120
  capability-based planning, 136–137
  choosing, 120
  CONOPS, 138
  executing, 120
  mission needs statement, 133
  operational planning model, 124–125
strengths in models, 124–125
strong passwords, 57, 220, 235
Stuxnet, 10, 37, 275–276
subject matter experts (SMEs), 161
subprime mortgage crisis, 218–219
supercomputing centers, 4
supply chains, 166, 170
Supreme Court, 268. *See also* judicial branch of government
survey designs, 288–299
  building models, 293–296

logit models, 292–293
NNSA example, 41–46
qualitative risk determination, 39–41
response rates, 42
sample populations, 289–290
statistical models, 290–292
SVs (schedule variances), 154–158, 163–164
symbols, fault tree, 52, 53
Syria, 276
systems, computer, 140, 182–184, 185, 195
systems of systems, 182–184, 187

T

t-test, 291
target audiences, 111, 112, 113
"targeted and actionable" warnings, 112–113
targets, 25, 27, 190, 202
tasks, 120, 148, 150
Taves, Kenneth H., 222–223
TCP/IP (Transmission Control Protocol/Internet Protocol), 187, 188, 189
technical audits, 167
technical guidance, 304
telephone surveys, 40
tensions
between military and civilian control, 70, 71, 78–81, 104–105
between security and freedom, 282
terminating sessions, 207
terrorism
aggravated identity theft, 273
board of directors role in prevention, 231–232
counterterrorism reviews, 100–101
international issues, 281
monitoring for, 204
Oklahoma City, 1995, 85–86
September 11th, 2001, 15–16, 129
in threat spectrum, 28
World Trade Center, 1993, 85
test groups, 247
test statistics, 290
testing
FISMA requirements, 98
hypotheses, 248–249
penetration testing, 234–235
risk research questions, 39
theories (cybersecurity research), 246
THOMAS.gov, 264
threat assessment
components, 25–28
DHS monitoring case study, 161–162
mission needs statements, 133
model corporate program, 232–233
threat environments, 133
threat shifting, 28
threat signature technology, 99–100
threats, 23, 25
analyzing consequences/vulnerabilities, 33–37
assessing. *See* threat assessment
attacks. *See* attacks and exploits
corporate governance and, 216
critical infrastructure focus, 87
espionage, 4
evolution in, 105
external, 28
factors aiding in, 202
growth in, 99
identifying, 38, 133, 205–208
increases in, 33
insider, 200, 233
internal, 28
malware, 195, 196, 271
risk assessment and, 23
in risk determination, 36
in risk equation, 23
in risk management framework, 16, 20
shared, 8, 87
signature technology, 99–100, 205, 206, 237–238
simulating, 206–207
spectrum, illustrated, 28
threat environments, 133
threat shifting, 28
worms. *See* worms
threshold values, 142–143
TIC Access Providers, 22
TIC (Trusted Internet Connection), 22, 138–139, 141, 258
time in budgets, 150–152
time-out tries, 295, 296
timelines, 120
TJ Maxx, 220
TJX data breach, 220, 226–227, 272
TLDs (top level domains), 192
tokens, security, 213
tolerances, risk, 16, 20, 21, 22
top-down analysis, 50–52
top level domains (TLDs), 192
total risk equation, 35
tracking projects
atypical variances, 302
comparing projects, 157–158
EVM budgeting, 153–158

EVM indexes, 298–300
over budget status, 163
red, yellow, and green status, 165
variances, significance of, 165
trade-offs
risk management framework, 16, 20, 21, 23
secure websites, 59
trade secrets, 233
training
corporate programs, 235
costs, 160
education as capability, 159
FISMA requirements, 98
health care systems, 224
transferring risks, 16, 20, 60, 61–62
Transmission Control Protocol (TCP/IP), 187, 188, 189
transnational issues. *See* global cybersecurity issues
transparency in corporate governance, 215
transportation systems, 85, 87, 96
travel costs, 146, 160
Treasury Department, 72
treaties, 284
trial courts, 268
trial-out tries, 295, 296
trials, 274
Trojan horses, 196
Truman administration, 128
trust, customers, 220, 238
trust protocols, 179, 188, 191–192, 198–199
Trusted Internet Connection (TIC), 22, 138–139, 141, 258
Trusted Internet Connections Initiative, 138–139, 258
Twitter phishing attacks, 197
Tyco, 230

U
unacceptable risks, 22
unauthorized access, 9
unclassified information, 79
unconstitutional regulations, 267–268
under budget status, 156
undesired events (probability analysis), 51
unfavorable variances, 155, 156, 158, 298, 299–300
unintentional threats, 25–26
United Kingdom cyber defenses, 37
United Nations cybersecurity efforts, 283
United State Sentencing Commission (USSC), 274
United States
government. *See* Federal government
government agencies. *See under* agency names (i.e., Defense Department, EPA)
Internet number registry, 278
Stuxnet virus, 10, 102, 275–276
United States v. Jones, 269
units of analysis, 248, 249
unknown vulnerabilities, 201–202
updating tools, 238
U.S. Attorneys, 273, 274
U.S. Computer Readiness Team (US-CERT), 122–123
U.S. Cyber Command, 73
US-CERT (U.S. Computer Readiness Team), 122–123
USB memory sticks, 185
"useful life," defined, 149
users
behavioral detection, 206
in cybersecurity operations, 202
numbers of, in modeling, 57, 295, 296
user-friendly websites, 58, 59
as vulnerabilities, 200
USNRC (Nuclear Regulatory Commission), 47, 53
USSC (United States Sentencing Commission), 274

V
validity tests, 249
values (binary code), 180
variables
logit models, 292
PRA risk management, 47
regression modeling, 56
research, 248
test statistics, 291
variances (EVM)
atypical, 302
comparing projects, 157–158
vs. EVM indexes, 298
favorable/unfavorable, 155, 156, 158, 298, 299–300
percentages, 157–158
significance of, 165
understanding, 154–158
variance triangle, 156
vendors/contractors
compliance, 168
cybersecurity operations, 202
health care systems, 224
IMS documents, 148
POA&M documents, 147–148
policies for managing, 238
PWS documents, 145
RFIs and, 143–144
RFP responses, 147–148
security breaches, 213

selection, 147–148
SOO documents, 146
threats resulting from, 233
vetoing
bills, 263
regulations, 267
victims, 273, 275
violating policies, 205–206
virus software. *See* antivirus software
viruses
capabilities, 196
Coreflood virus, 198
criminal prosecution, 271
Flame, 102, 276
government efforts to focus on, 87
Stuxnet, 10, 102, 275–276
viva voce, 263
voicemail hacking, 5
volatile memory, 184–185
volunteer sampling, 289–290
voting, 263
vulnerabilities, 23, 195–196
analyzing threats/consequences, 33–37
assessing, 23, 29–30, 161–162, 232, 233
BGP, 191–192
complexity of systems and, 184
corporate governance and, 216
databases of, 201
DHS monitoring case study, 161–162
hash detection methods, 195
human, known, and unknown, 200–202
identifying, 38
increases in, 33
Internet, 179
IP addresses, 190
mainframes, 76
"National Strategy to Secure Cyberspace," 95
personal computers, 78–80
public-private shared research, 87
risk determination, 36
risk equation, 23
risk management framework, 16, 20
trust protocols and, 188
vulnerability assessments, 23, 29–30, 161–162, 232, 233

W

WANs (wide area networks), 188
War Games, 6
Warner Amendment, 81
warning systems, 110–113
as capability, 203, 207
effectiveness, 112
as high-level requirement, 136
importance of warnings, 111
management, 110–113
too many warnings, 112, 113
US-CERT failure, 122–123
water systems, 87, 96
WBS (work breakdown structure), 146, 148, 160
weaknesses. *See* vulnerabilities
websites
cyber attacks, 276
District Design. *See* District Design case study
DNS cache poisoning, 200
encrypting, 194
fraudulent credit card usage, 222
history of, 185–186
phishing attacks, 197–198
White House, 259, 276. *See also* EOP; presidents
wide area networks (WANs), 188
WiFi networks, 198, 227
wireless systems, 198, 227
Wiretap Act, 272
work breakdown structure (WBS), 146, 148, 160
Working Group on Web Security, 280
World Summit on the Information Society (WSIS), 283
World Trade Center attacks
1993, 85
2001, 15–16, 90–99, 129, 257
World Wide Web, 9, 185–186
WorldCom, 168, 230
worms
capabilities, 196
criminal prosecution, 271
Flame, 102, 276
Morris, 8–9, 270
Stuxnet, 10, 102, 275–276
written cybersecurity plans, 234
WSIS (World Summit on the Information Society), 283

Y

Y2K preparations, 89
yellow project status, 165

Z

z-test, 291
zero-day exploits, 195, 201–202, 206
zombie networks, 198