Index

Page references in italics refer to figures.

A

“absurdity test,” 144
Adobe, 260–263, 263
Advanced Data Stealing Threat
(ADST) (dimensional modeling use case), 221, 221–224, 222–223
“Aggregating Data Sources for Cyber Insights” (Lipkis, Chan, Lee), 250–254, 251, 252, 253, 254
AIR Worldwide, 266–267
alpha distribution parameters
beta distribution, overview, 243–244, 245
beta distribution case (AllClear ID), 178 (See also beta distribution parameters)
overview, 171–172, 172, 173, 175–176
SDA example model (R programming), 208, 209, 210
truncated power law and, 245, 246
“analysis placebo,” 57–59
analytics technology, building, 232. See also business intelligence (BI)
anchoring, 70–71, 144
Andreassen, Paul, 58
Anthem, 124
Aon, 103
APIs (application program interfaces), 214
Armstrong, J. Scott, 75, 119
assets
at-risk value of assets, 250
dimensional modeling example, 222
“assumptions,” avoiding, 147
attack surface, defined, 8–11
Attitudes Toward Quantitative Methods (ATQM) (survey), 81–83, 82
audits, 232–233, 234–236

B

Bayes, Thomas, 25, 157
“Bayesian” interpretation, 149
Bayesian methods, 157–168, 169–196
applying, 195–196
Bayes and probability theory, overview, 161–165, 165
Bayes triplot and beta select function, 208–210, 209, 210
Bayesian methods (continued)
binary terms, defined, 160
estimating value of information for cybersecurity, 190–193, 191
Lens method, 184–190, 186
leveraging existing resources to reduce uncertainty, 193–195, 195
log odds ratio (LOR) method, 180–184
major data breach example, 158–160, 165–168, 166
node probability table (NPT), 178–180
overview, 24–26, 157–158
prescriptive analytics example, 206–211, 209, 210
betadist (Excel function), 171, 172
beta distribution parameters applying beta to breaches, 174–176, 175
Bayes triplot and beta select function, 208–210, 209, 210
calculations with, 171–174, 172, 173
case study (AllClear ID), 177–178
computing frequencies with, 170–171
defined, 243, 243–244
effect of, 176–177, 177
overview, 171, 172
reducing uncertainty and, 190, 193
betainv (Excel function), 244
beta.inv (Excel function), 171, 176
beta.par (R function), 208, 209, 210
beta.select (R function), 208, 209
BI. See business intelligence (BI)
Bickel, J. Eric, 93–95
“big data” solutions, 200
binary distribution, 240, 240–241
binary terms, defined, 160
binomdist (Excel function), 173, 176
Bohn, Christopher “Kip,” 103
botnets, 255–259, 256, 257, 258
Box, George, 96
Bratvold, Reidar, 93–95
breach “cascade,” possibility of, 11
Breach Portal (U.S. Department of Health and Human Services), 194
Brunswik, Egon, 184–185
budgets for cybersecurity, since September 11, 2001, 12
“Building Acceptance for Better Methods” (Jones), 107–109
“Bunch of Guys Sitting Around Talking” (BOGSAT) method, 74
business intelligence (BI), 213–227
addressing concerns about, 215–216
dimensional modeling, overview, 214, 214, 216–221, 217, 218, 219, 220
dimensional modeling use case, 221, 221–224, 222–223
measuring people-based processes, 225–227, 226
overview, 213–214
C
calibrated estimates, 133–155
calibration exercise, 137–143, 138–139, 140, 142
calibration exercise, 137–143
conceptual obstacles to calibration, 145–150
effects of calibration, 150–154, 152
overview, 38, 133
repetition and feedback for, 143–144, 145
subjective probability, 134, 134–137
catastrophe modeling, applying to cyber risk, 266–268, 267
cbind (R function), 210
CFO Magazine, 12
“chain rule tree,” 164–165, 165
Chan, Chuck, 250–254, 251, 252, 253, 254
chief financial officers (CFO), 67
chief information officers (CIO), 151
chief information security officers (CISO)
collaboration component, 74
decompensation component, 75–76
executive-level attention needed for cybersecurity, 12, 229–233, 231
expert consistency component, 69–73, 72, 73
expertise of, for quantitative risk assessment, 37–38, 53–54
statistical models versus expertise, 61–65
tools for improving human component, 66–67
chief technology risk officers (CTRQ), 230, 232
Cl. See confidence intervals (CI)
CIA, 86, 87
clarity
clarification chain, 27–28
for decision analysis, 119–120
Clinical versus Statistical Prediction (Meehl), 62–63
Clinton, Jim, 100
cloud breach (example), 158–160, 165–168, 166
collaboration component, 74
Comey, James B., 7
Common Configuration Scoring System (CCSS), 92
Common Vulnerability Scoring System (CVSS), 14, 92
Common Weakness Scoring System (CWSS), 92
concept of measurement, 19, 20–26
confidence intervals (CI), 79n22, 135, 137–143, 138–139, 140, 142. See also calibrated estimates
confidentiality, integrity, availability (“C, I, A”), 114–116, 115, 117
configuration (dimensional modeling example), 223
consistency, 69–73, 72, 73
continuous integration and continuous development (CICD), 225
continuous probability distribution, 134, 134
countif (Excel function), 48
countifs (Excel function), 192
coupons, predictions about, 80n33
coverage and configuration metrics, 202
Cox, Tony, 89–92, 235
CSRM. See cybersecurity risk management (CSRM)
C-Suite decisions, about cybersecurity risk management, 12, 229–233, 231
cumulative probability function (CPF), 46, 171, 172, 173
CVSS. See Common Vulnerability Scoring System (CVSS)
“Cyber-Cl” (Samuelson), 264–265
cybersecurity
Attitudes Toward Quantitative Methods (ATQM) (survey), 81–83, 82
Bayesian methods, 190–193, 191
budgets for, since September 11, 2001, 12
catastrophe modeling, 266–268, 267
chief information security officers (CISO), 12, 229–233, 231
cybersecurity (continued)
financial impact of cyber incidents, 250, 253, 253–254
frequency of cyber incidents, 250, 252, 252–254, 253
risk measurement obstacles, 81–83, 82
Target cybersecurity breach example, 9, 11, 12, 103–105, 23
See also Bayesian methods; calibrated estimates;
cybersecurity risk management (CSRM); decomposition;
measurement, overview; measurement of risk analysis methods; security metrics maturity
cybersecurity risk management (CSRM), 229–238
audits for, 234–236
for avoiding widespread problems, 237–238
establishing strategic charter for, 229–233, 232
global attack surface, defined, 8–11
organizational roles and responsibilities for CSRM, 231, 231–233
overview, 7–8
proposal for, 15–17
response to, 11–15, 13
support needed for, 236–237

D
data, resources for, 59–61
Dawes, Robyn, 62, 63–64
DBIR. See Verizon Data Breach Investigations Report (DBIR)
decision analysis
about decomposition, 75–76, 113, 119–120
audits for, 232–233, 234–236
calibration and probabilistic analysis in decision making, 153–154
at executive level, 229–233, 231
improving, 1–3
measuring risk analysis methods and, 62–65
decomposition, 113–131
of one-for-one substitution model, 114–118, 115, 116
overview, 75–76, 113
reputation damage, 124–129, 125, 126
rules of, 122–123
variation of strategies for, 118–122
descriptive analytics, 204–205
dimensional modeling
defined, 214, 214
producing data marts with, 216–221, 217, 218, 219, 220
use case, 221, 221–224, 222–223
discont (R function), 210
discrete binary probability distribution, 134, 134
distributions (select), 239–246
beta, 243, 243–244
binary, 240, 240–241
lognormal, 242, 242–243
normal, 241, 241–242
power law, 244, 245
triangular, 239, 239–240
truncated power law, 245, 245–246
“duplicate pair” method, 186
E
Economics & Management (Society of Petroleum Engineers), 93
EOL (Expected Opportunity Loss), 190
equivalent bet test, 141
espionage attacks, forecasting and reducing, 250–252, 251
ETLs (Extraction, Transformation, Load), 215
Evans, Dylan, 93
EVPI (Expected Value of Perfect Information), 190
Excel/Excel functions
betadist, 171, 172
betainv, 244
beta.inv, 171, 176
binomdist, 173, 176
countif, 48
countifs, 192
Data Table function to process SIPs, 256–257, 257
generating random events and impacts in, 40–45, 41, 43, 44
lognorm.inv, 42, 243
min, 43
normdist, 40
norminv, 41, 242
rand, 40, 41, 42, 45, 115, 240, 241, 242, 243, 244, 258
spreadsheet examples, 40
executive-level decisions, about cybersecurity risk management, 12, 229–233, 231
Expected Opportunity Loss (EOL), 190
Expected Value of Perfect Information (EVPI), 190
expert consistency component, 69–73, 72, 73
Expert Political Judgment (Tetlock), 63
“Exsupero Ursus” fallacy, 96–97

F
Factor Analysis of Information Risk (FAIR) method, 53–54
facts (measures), 219
Failure of Risk Management, The (Hubbard), 85, 103
FBI, 7–8
Fear, Uncertainty, and Doubt (FUD), 7–8
feasibility, of quantitative methods, 97, 97–99, 98
feedback, 65, 143–144, 144
financial impact, of cyber incidents, 250, 253, 253–254
firewalls (FW), 47, 65, 193, 202, 219, 223
“Flaw of Averages in Cyber Security, The” (Savage), 255–259, 256, 257, 258
“flip,” Bayes’s rule, 162–163
Forbes, 9, 124, 127
Fox, Craig, 89
frequency, of cyber incidents, 250, 252, 252–253, 253
“frequentist” interpretation of confidence intervals, 149
Freund, Jack, 53–54
“full metal jacket,” 217–218
functional security metrics (FSMs), 199, 201–202

G
Gartner, Inc., 10
Geer, Daniel E., ix–x
GE Healthcare, 194, 260–263, 263
Giga Information Group, 151–153
global attack surface, defined, 8–11
Global Information Security Workforce Study (GISWS), 9
Graves-Morris, Peter, 94
<table>
<thead>
<tr>
<th>Index</th>
</tr>
</thead>
</table>
| **H** hardening, of systems, 11–12  
*Harvard Business Review*, 25–26  
healthcare industry, data breaches in, 252, 252–253, 253  
Heat Map Theory and Empirical Testing, 94, 94  
Heuer, Richards, J., Jr., 86, 87, 235  
HITECH Act, 252  
Home Depot, 125, 125–128, 126  
Host Intrusion Prevention (HIPS), 193, 203, 223  
Howard, Ron, 25–26, 119–120  
“How Catastrophe Modeling Can Be Applied to Cyber Risk” (Stransky), 266–268, 267  
*How to Measure Anything* (Hubbard), 1, 19, 31, 33, 51, 133, 136–137, 189  
Hubbard, Douglas W.  
on calibrating people, 150  
clarification chain, 27–28  
on equivalent bet test, 141  
The Failure of Risk Management, 85, 103  
*How to Measure Anything*, 1, 19, 31, 33, 51, 133, 136–137, 189  
research by, on Target cybersecurity breach, 104  
subjective probability component  
research by, 68–69  
Hubbard Decision Research, 83, 100  

**I** IBM Journal of Research & Development (Evans), 93  
in illusion of communication, 85–89, 105–106  
InfoLogix, 264–265  
Information Systems Audit and Control Association (ISACA), 82  
information technology (IT) industry, 12, 21–22, 27, 29, 61, 151, 152, 251. See also cybersecurity risk management (CSRM)  
information theory, 21–22  
informative decomposition, 121  
inherent risk, 47, 47–50, 49  
insider threats, identifying, 264–265  
intellectual property (IP), 1, 8, 114, 117, 144, 179  
Intergovernmental Policy on Climate Change (IPCC), 86, 87  
International Organization for Standardization (ISO), 85  
Internet, increased use of (2001 to 2014), 10  
Internet of Things, 10  
Interval measurement scales, 23–24  
investment, probability example of, 58  

**J** Jaquith, Andrew, 201, 214, 267  
JCPenney, 125, 125–128, 126  
Jensen’s Inequality, 255  
Jones, Jack, 53–54, 107–109  
JPMorgan, 12  
junk dimensions (dimensional modeling example), 222  

**K** Kahneman, Daniel, 64, 68, 97, 135–136  
key performance indicators (KPI), 201  
Kuypers, Marshall, 128, 194–195  

**L** LB. See lower bound (LB)  
Lee, Thomas, 250–254, 251, 252, 253, 254
measurement, overview, 19–34
concept of, 19, 20–26
defined, 21–22
methods of measurement,
defined, 19–20, 30–34
object of, 19–20, 26–30
overview, 19–20
of risk, defined, 29
of uncertainty, defined, 29
measurement of risk analysis
methods, 55–80
“analysis placebo,” 57–59
collaboration component, 74
data resources for, 59–61
decompensation component,
75–76
expert consistency component,
69–73, 72, 73
improving expertise for, 66–67
overview, 55–56
statistical models versus expertise
for, 61–65
subjective probability component,
67–69
measures (facts), 219
Meehl, Paul, 62–63, 76
Metropolis, Nicholas, 39
min (Excel function), 42, 243
Monte Carlo simulation
measuring risk analysis methods,
63
overview, 36, 39–45, 41, 43, 44,
48, 52, 53

N

NASA, 63, 95
National Bureau of Economic
Research, 67–68
National Institute of Standards and Technology (NIST), 14, 237
National Security Telecommunications, 10
NATO, 86, 87
Network Intrusion Prevention Systems (NIPS), 193, 223
node probability table (NPT), 178–180
nominal measurement scales, 23–24
normal distribution, 40–43, 41, 241, 241–242
normdist (Excel function), 40
norminv (Excel function), 41, 242
Nuclear Regulatory Commission (NRC), 66

O
object of measurement, 19–20, 26–30, 113. See also decomposition observability, for decision analysis, 116–118, 119–120
oil industry, quantitative methods used by, 61, 63, 71, 83, 92, 93, 95, 103, 105, 109, 138
one-for-one substitution model decomposition of, 114–118, 115, 116
overcoming objections with, 105–106
overview, 36, 36–37
subjective probability and, 134, 134–137
Online Analytical Processing (OLAP), 205
“On the Theory of Scales and Measurement” (Stevens), 23–24
open source solutions, 215
Open Web Application Security Project (OWASP), 14, 84, 92, 120
operational security metrics maturity model, 199, 200, 200
ordinal measurement scales defined, 23–24
as measurement obstacle, 83, 100–103
psychology of scales and illusion of communication, 85–89
overconfidence, 68–69, 136, 143
“over-decomposition,” avoiding, 120–122

P
“Password Hacking” (Mobley), 260–263, 263
passwords, 194
pattern-analysis methods, 264–265
payment card industry (PCI), 118, 135, 179, 233
pbetap (R function), 210
penance projects, 128–129
people processes, dimensional modeling for, 225–227, 226
personal health information (PHI), 118, 135, 260
Poneman Institute, 124
positive pen test (PPT), 160
power law distribution, 244, 245
power law distribution, truncated, 245, 245–246
predictive analytics, 199, 205
pred.probs (R function), 210
prescriptive analytics, 199, 204–211, 209, 210
Princeton University, 261
prior probabilities (priors), 157, 164
probability
as Bayesian interpretation, 24–26
cumulative probability function (CPF), 46, 171, 172, 173
measurement risk of, 100–103
probability density function (PDF), 172
probability theory definitions, 161–163
program management, 232–233, 234–236
psychological diagnosis, probability example of, 58
Psychology of Intelligence Analysis (CIA), 86, 87

Q
qbeta (R function), 210
quantile (R function), 210
quantitative risk analysis (QRA), 35–54
CISO expertise and, 37–38, 53–54
feasibility of quantitative methods, 97, 97–99, 98
Monte Carlo simulation, 36, 39–45, 41, 43, 44, 48, 52, 53
one-for-one substitution versus risk matrix, 36, 36–37
overview, 35
quantitative expression, 22
quantitative risk analysis (QRA), 231, 231–233
supporting decision for, 51–53
visualizing risk, 46, 46–51, 47, 49

R
rand (Excel function), 40, 41, 42, 45, 115, 240, 241, 242, 243, 244, 258
range compression, 90, 90–92
ratio measurement scales, 23–24
rbeta (R function), 210
regression analysis
  Lens method and, 184–187, 186
  Lens method versus LOR, 187–189
logistic regression, 180
“softer” methods and, 95
relational database management system (RDMBS) technology, 203, 215
remotely exploitable vulnerability (REV), 159, 160–164, 167, 202
reputation damage examples, 124–128, 125, 126
penance projects, 128–129
residual risk, 47, 47–50, 49
return on risk mitigation, 8
reuse rate, for passwords, 260–263
R functions
  beta.par, 208, 209, 210
  beta.select, 208, 209
  cbind, 210
discint, 210
  pbetap, 210
  pred.probs, 210
  qbeta, 210
  quantile, 210
  rbeta, 210
  triplot, 209, 209, 210
risk, defined, 29
risk matrix
  amplifying effects of, 92–95
  ending promotion of, 236
  as measurement obstacle, 84–95, 87, 90, 94
  one-for-one substitution versus, 36, 36–37
  overview, 13, 13–15
risk matrix theorem, 89–92
risk measurement obstacles, 81–110
“Building Acceptance for Better Methods” (Jones), 107–109
communication and consensus objections, 105–106
“Exsupero Ursus” fallacy, 96–97
feasibility of quantitative methods and, 97, 97–99, 98
risk measurement (continued)
interview of cybersecurity professionals, overview, 81–83, 82
ordinal scales, 83, 100–103
of risk matrix, 84–95, 87, 90, 94
statistics literacy and acceptance, 99–100
Target cybersecurity breach example, 9, 11, 12, 103–105, 238
risk metrics, functional security metrics (FSMs) and, 202
“risk/return” tradeoffs, 51
risk tolerance curve, 47, 47–49, 50–51
RockYou, 261–262
R programming language (prescriptive analytics example), 206–211, 209, 210
Rule of Five, 33

S
Sample size, 30–34
Samuelson, Doug, 264–265
Savage, Sam, 255–259, 256, 257, 258
scoring systems, 13–15
SDA. See sparse data analytics (SDA)
security data marts (SDM), 199, 202, 203–204
security facts, 219
security information and event management (SIEM), 12, 204
Security Metrics (Jaquith), 201, 214
security metrics maturity, 199–211
functional security metrics, 201–202
operational security metrics maturity model, 200, 200
predictive analytics for, 199, 205
prescriptive analytics, 204–211, 209, 210
security data marts, 203–204
sparse data analytics, 201
Seiersen, Richard, 104, 194
September 11, 2001 terrorist attacks cybersecurity budgets and, 12
security response following, 7
Shannon, Claude, 21–22
simulated realizations (SIPs), 256, 256–259, 257, 258
Society for Information Risk Assessment (SIRA), 82
Society of Petroleum Engineers, 93
sparse data analytics (SDA), 199, 201, 206–211, 213
sports, probability examples, 57–58
Standard 31010 (International Organization for Standardization), 85
standards organizations, on risk matrix, 14, 85, 236–237
Stanford University, 25–26, 94, 128, 255–259, 256, 257, 258
statistical significance, 30–32
statistics literacy, attitudes about, 97, 97–100, 98
Stevens, Stanley Smith, 23–24
Stochastic Information Packets (SIPs), 256–258, 268
Stransky, Scott, 266–268, 267
Strategic Decision and Risk Management (Stanford University), 94
Structured Query Language (SQL), 8, 215–216
subjective probability
importance of, 67–69
misconceptions about, 145–150
overview, 35, 134, 134–137
Surowiecki, James, 74
survey(s)
Attitudes Toward Quantitative Methods (ATQM), 81–83, 82
calibrated estimates, 148
communication and consensus objections, 105–106
decomposition, 127
defined, 21
feasibility of quantitative methods, 97–100, 101
methods based on Bayes, 169, 185, 194
methods of measurement, 30–32, 73
reputation damage and, 124
risk matrices, 84, 86, 89
rolling out cybersecurity risk management, 237
survival analysis, 204, 221, 221–222

T
Target
avoiding similar cybersecurity attacks, 238
decomposing reputation damage to, 124–128, 125, 126
overview of cybersecurity attack, 9, 11, 12, 103–105
“Target Says Data Breach Hurt Sales, Image” (Forbes), 124
Tetlock, Philip, 63
Thomas, Philip, 93–95
thought experiments, clarification chain and, 28
threat intelligence/threat management, 12
T.J. Maxx, 127–128
training
building, 232
calibrated estimates and, 151
Trefis, 124, 127
triangular distribution, 239, 239–240

triplot (R function), 209, 209, 210
trivia, probability example of, 58
truncated power law distribution, 245, 245–246
Tuft, Edward, 94
Tversky, Amos, 64, 68, 135–136

U
UB. See upper bound (UB)
Ulam, Stanislaw, 39
uncertainty, defined, 29
uncertainty reduction, measurement as, 24
“uninformative decomposition,” 121
University of California - Los Angeles (UCLA), 89
University of Chicago, 57–58
University of Michigan, 62
upper bound (UB), 38, 41–43, 43, 67, 101, 115, 122, 137, 138, 144
U.S. Department of Health and Human Services, 194, 252
U.S. Department of Veteran Affairs, 27, 146–147
usefulness, for decision analysis, 119–120
U.S. Senate Committee on Homeland Security and Governmental Affairs, 7

V
Verizon Data Breach Investigations Report (DBIR), 251
Visa, 104
Vivosecurity, 194, 250–254, 251, 252, 253, 254
von Neumann, John, 39
vulnerability
  increase of, 11
vulnerability dimension
  (dimensional modeling example), 223
vulnerability management, 12

Wisdom of Crowds, The
  (Surowiecki), 74

X
  XL Catlin, 9

Y
  “Year of the Data Breach, The”
    (Forbes), 9

Web Application Firewalls (WAF),
  223