Index

A

ability, 42–44
accounting practices, 37–39
Acer ransomware attack, 224
active communication tools, 92, 93–94
  adjusting, 155–156, 159–160
  CBT, 102–103
  contests, 103, 160, 218
  engagement metrics, 111–112
  events, 103–105
  hidden costs, 94, 101–102
  knowledgebase, 95–96
  outside speakers, 104–105
  posters, 96–97
  quarterly delivery schedule, 133–136
Active Directory (AD), 192–193
ad hoc gamification, 174
advertising campaigns, 24–26
advocacy group interviews, 68, 247–248
adware, 9–10
Amazon Echo, 83
ambassadors, 209–210
  adding, 160
  as communication tool, 90–92
  winning support via, 218
Android phones, 96
annual programs, 131–133
antecedents, 41–42, 166–167
antimalware software, 29–30
antivirus software, 9
approvals, 146–147
assets, 46–50
attendance metrics, 111–112
auditors
  Check-the-Box requirements, 20–21
  compliance requirements, 109–110
  security culture, 64–65
authentication security checks, 21
awareness. *See also* security awareness programs
  ABCs of, 39–40, 166–167
  advertising/marketing versus, 24–26
  countermeasure messages, 49
  goal of, 9–10
  index scores, 152–153
  role of, 7, 15–16, 31

B

backup generators, 49
badges, 40, 41, 114
  NSA example, 11–12
  observing user behaviors with, 114
  organizational culture, 62, 64
  physical security, 81
  tailgating exercises, 148, 172
Baltimore (MD) ransomware attack, 224
bank account security, 82
basic computer security
  executive awareness program, 131
  as program topic, 80, 81, 85, 223
behavior modification
  goal of security awareness programs, 11–13, 14
  motivating users to do thing right, 77–79
  security as a must-do task, 21–23
  tracking
    gamification, 115–116
    incidents, 113–114
    overview, 113
    simulations, 114–116
behavior points, 178
behavioral metrics, 113, 156–157
  Day 0 metrics, 118, 138
  gamification, 115–116
  incidents, 113–114
  simulations, 114–116, 183–184

COPYRIGHTED MATERIAL

behavioral science, 33
ABCs, 41–42, 166–167
accounting practices, 37–39
awareness ABCs, 39–40
common knowledge/sense, 34–35
group psychology
B:MAP model, 42–44
Fogg Behavior Model, 42–43
Forgetting Curve, 44–45
overview, 40–41
psychology versus, 23–24
risk management
optimizing risk, 46
overview, 45–46
risk formula, 46–50
safety science
overview, 35
recognizing incidents as system failures, 36
responding to incidents, 37
behaviors
ABCs of, 41–42, 166–167
awareness ABCs, 39–40
B:MAP model, 42–44
black bag operations, 1
B:MAP model, 42–44
Booz-Allen, 48
bots, 81
branding, 139–141, 146–147
Brazil, 87
breaking news items, 161–162
bring-your-own-device (BYOD) programs, 174, 212
Brown, Tracy Celaya, 10
budget/funding, 13
additional sources, 123–125
choosing number of programs, 127–129
compliance budget concept, 22–23
compliance requirements, 20–21, 102, 109–110
constraints, 125
corporate communications department, 124
determining actual, 122–123
hidden costs, 94, 101–102
increased, 122
limiting discretionary budget, 126
metrics
behavior tracking, 113–116
Day 0, 29, 118, 138
engagement, 111–113
hidden costs, 108–109
not collecting, 29
overview, 12–13, 59, 107, 110
ROI, 116–117
strategy planning, 54, 57–58
tracking intangible benefits, 117
vendor tools, 108, 144–145
phishing simulations, 122, 125, 136–137
staff considerations, 126
strategy, 58–59
business drivers. *See also* organizational culture
gamification, 174
personal awareness, 76–77
in strategy planning, 54, 61, 65
subcultures, 55–56, 65–66
topics based on, 56–57, 76
business email compromise, 222
BYOD (bring-your-own-device) programs, 174, 212

C

cables, 83
camera covers, 101
campaigns. *See* phishing simulations
carelessness, 47
catchphrases, 140
caution
with FUD factor, 218–219
phishing simulations, 131, 191, 199–200
CBT. *See* computer-based training
cellphone chargers, 177
CEO (chief executive officer), 67, 69, 70
certificates, 177
champions, 209–210
adding, 160
as communication tool, 90–92
winning support via, 218
cheat sheet, 3
cheating, 198

Check-the-Box requirements, 20–21
CBT, 102
mandated tools, 125
metrics, 109–110
phishing simulations, 183
chief executive officer (CEO), 67, 69, 70
chief experience officers (CXOs), 69
chief information security officer (CISO), 20
interviewing
overview, 70, 71
sample interview questions, 234–247
phishing simulations, 185
children, protecting, 76, 85
China, 9
clean desk drops, 171–172
clothing items, 177
cloud security, 82
Cofense software, 188
coffee cups, 99–100
Colonial Pipeline ransomware attack, 9
common knowledge/sense, 34–35
communications department, 64
budget/funding, 124
interviewing, 68, 250
logistics, 145
phishing simulations, 185
communications tools, 24
active
CBT, 102–103
contests, 103, 160, 218
events, 103–105
hidden costs, 101–102
knowledgebase, 95–96
outside speakers, 104–105
overview, 92, 93–94
posters, 96–97
adjusting, 155–156, 159–160
choosing, 62–63
common knowledge/sense, 34
engagement metrics, 111–112
interviewing stakeholders
contact information, 72
general questions, 71
intangible benefits, 117
interview content, 70–72
overview, 67
scheduling, 70
whom to interview, 67–70
partnering, 72–73
passive
camera covers, 101
coffee cups, 99–100
design styles, 93
desk drops, 72, 99, 171–172
monitor displays, 89, 97–98, 100
mousepads, 100
other giveaways, 100–101
overview, 92–93, 95
pamphlets, 98
pens, 100–101
printed newsletters, 54, 55, 97, 133–136
screen savers, 98
sleeves, 99–100
squishy toys, 101
stickers, 100
table tents, 99, 133–136
quarterly delivery schedule, 133–136
security ambassadors, 90–92
sources/vendors, 108, 144–145
staff considerations, 126
in strategy planning, 54, 55–56
compliance budget concept, 22–23
compliance programs
communications tools advice, 95
interviews
overview, 68
sample interview questions, 234–247
metrics reporting, 149
as program topic, 87
compliance requirements
budget/funding, 20–21, 102, 109–110
CBT, 102
mandated tools, 125
metrics, 109–110
phishing simulations, 183

compliance standards, 21–23
computer security
executive awareness program, 131
as program topic, 80, 81, 85, 223
computer-based training (CBT), 29
budget/funding, 122, 125
as communication tool, 102–103
hidden costs, 94
LMS, 111–112
phishing simulations, 189–190
quarterly delivery schedule, 133–136
as tactic, 53
consequences
behavioral science ABCs, 41–42, 166–167
B:MAP model, 43–44
gamification, 166–167
contests
adding, 160
as communication tool, 103
winning support by hosting, 218
cooking the books, 198
corporate communications department, 64
budget/funding, 124
interviewing, 68, 250
logistics, 145
phishing simulations, 185
corporate culture. *See* culture; organizational culture
corporate wellness programs
communications tools advice, 95
interviewing, 68–69, 247–248
support for awareness programs, 214
countermeasures
for "gaming the system," 14
purpose, 169
in risk formula, 46–47, 49–50
counterterrorism campaigns, 24
COVID-19 pandemic
communications tools after, 63
impact on awareness programs, 162–164
phishing attacks, 198
program delivery scheduling, 132
travel security, 83
WFH security during, 84
credentials, 9
awareness ABCs, 39–40
as awareness topic, 82, 223
common knowledge/sense, 34
observing user behaviors with, 114
in risk formula, 47
strength, 162, 167
credit card rewards, 87, 166
crowd behaviors, 33
accounting practices, 37–39
awareness ABCs, 39–40
common knowledge/sense, 34–35
group psychology
behavioral science ABCs, 41–42
B:MAP model, 42–44
Fogg Behavior Model, 42–43
Forgetting Curve, 44–45
overview, 40
risk management
optimizing risk, 46
overview, 45–46
risk formula, 46–50
safety science
overview, 35
recognizing incidents as system failures, 36
responding to incidents, 37
culture
awareness ABCs, 39–40
behavioral science ABCs, 41–42, 166–167
B:MAP model, 42–44
consequences, 42
determining, 64–65
Fogg Behavior Model, 42–43
Forgetting Curve, 44–45
organizational culture versus, 55, 62, 64–65
in strategy planning, 54
tracking intangible benefits, 117
cup warmers, 83
custom phishing tools, 187–189
CXOs (chief experience officers), 69
Cyber Security Body of Knowledge (CyBOK) project, 230

cyberhygiene, 28, 80, 81, 85
Cybersecurity Awareness Month, 76
Cybersecurity Culture Guidelines, 229
cybertheft, 34–35
CybSafe Research Library, 228

D

data backups, 48
data privacy, 83, 87
Day 0 metrics
  budget/funding, 29, 118, 138
  logistics, 147–148
  phishing simulations, 194–195
DBIR (Verizon Data Breach Investigations Report), 3, 9, 85
decision trees, 14
Dekker, Sydney, 230
design styles, 93
desk drops, 72, 99, 171–172
digital picture frames, 83
distribution resource partnerships, 73
DLP software, 114
domains, 194
drive encryption, 81
dumpster diving, 26, 80

E

e-commerce account security, 82
email compromise, 222
email gateway, 122, 125
email messages
  common knowledge/sense, 34
  phishing attacks, 8–11
  phishing simulations, 182, 187
emergency responders, 37
engagement metrics, 111, 138
  attendance, 111–112
  intangible benefits, 149
  knowledge, 112–113
  likability, 112
  proper use, 155–156
escape rooms, 103, 218
ethical considerations, 131, 191, 199–200
European Union Agency for Cybersecurity (ENISA), 229
events
  as communication tool, 103–105
  event tables, 160
  quarterly delivery schedule, 133–136
  winning support by hosting, 217, 218
executive awareness program
  increased funding, 122
  program support, 211, 215–216
  security awareness programs, 129–131
executive recognition, 177
executives, 67, 69, 70
experiential engagement, 160

F

Facebook, 86
fans, 83
fear, uncertainty, doubt (FUD) factor, 213, 218–219
firewall software, 29–30
first aid kits, 37
first responders, 37
Fogg, BJ, 22, 42
Fogg Behavior Model, 42–43
Forgetting Curve, 27, 44–45
  gamification, 166–167
  quarterly programs, 133
  topic distribution, 133–136
free phishing simulation software, 137
frequent flier programs, 58, 166
FUD (fear, uncertainty, doubt) factor, 213, 218–219
fun giveaways, 100–101

G

games, 101, 166–167
gamification program, 4, 165
  ad hoc, 174
  adding, 160
  awareness program support, 218, 219
  behavioral metrics, 115–116

gamification program *(continued)*
consequences, 166–167
examples
desk drops, 72, 99, 171–172
phishing attack reporting, 170–171
reporting security incidents, 173
tailgating exercises, 172–173
USB drop reporting, 173
Forgetting Curve, 166–167
four attributes, 168–169
full-scale implementation
behavior points, 178
reward tiers, 175–177
tracking users and points, 179
valid rewards, 177
phishing simulations, 201–202
Pokémon Go example, 176
promoting, 179–180
in strategy planning, 54, 58
tracking tools, 179
types of, 166–167
understanding, 165–167
where to implement, 169–170
"gaming the system," 14
GDPR, 87
general counsel
approvals, 146–147
budget/funding, 13
interviewing, 68, 247–248, 249
phishing simulations, 185
general project management, 146
geographic considerations
interviews, 69, 247–248
multiple awareness programs, 127–129
security awareness programs, 66
simulations, 115–116, 193
geotags, 86
gift cards, 177, 218, 219
giveaways, 100–101, 177, 218, 219
goals
establishing and measuring, 11–14
phishing simulations, 183–185, 194
unrealistic, 28–29
GoDaddy phishing simulation, 147, 191, 200
Google, 83, 201
GoPhish software, 137, 189
graphical dashboards, 149–151
grocery store frequent shopper programs, 166
group psychology, 40
behavioral science ABCs, 41–42, 166–167
B:MAP model, 42–44
Fogg Behavior Model, 42–43
Forgetting Curve, 44–45

H

hacking
focusing on doing work right rather than on, 77–79
Microsoft Exchange Server, 199
North Korea, 162
Ring cameras, 39–40
SolarWinds Orion, 199
Twitter, 49, 76, 162
vishing attacks, 76, 162
hardcopy newsletters
as communication tool, 97
quarterly delivery schedule, 133–136
in strategy planning, 54, 55
Hastings, Reed, 86
Hayden, Lance, 230
healthcare data regulation, 87
hidden costs, 94, 101–102, 108–109
HIPAA, 87
hiring managed services, 192, 197, 199
holiday message scams, 79
home network security, 131, 223
hot cup sleeves, 99–100
hotspots, 84
How to Run a Security Awareness Program course, 231
human error, 47
Human Factor Knowledge Area paper, 230
human firewall myth, 16–17, 122, 210
human resources (HR) departments, 13, 68, 185, 249
Human Security Engineering Consortium, 231
hurricanes, 49

I

icons, 3
identity theft, 77
"if you see something" campaign, 24, 25
ignorance, 47
incidents, 35
  behavioral metrics, 113–114
  including as topics, 161–162
  increased funding due to, 122
  as program topic, 225
  report gamification, 173
  responding to, 37
  in strategy planning, 54
  as system failures, 36
index scores, 152–153
individual psychology, 23–24
Industry Sharing and Analysis Centers (ISACs), 162
influencers, 69, 216, 247–248
information technology (IT) departments, 185
information-action fallacy, 22
injuries, 35
  including as topics, 161–162
  increased funding due to, 47
  phases, 36
  recognizing as system failures, 36
  report gamification, 173
  responding to, 37
  as security awareness program topic, 225
  in strategy planning, 54
insider threats, 85
Instagram, 86
instant messaging security, 80
intangible benefits, 117, 149
interdepartmental partnering, 72–73
international credit card processing standard, 87
international cybersecurity standard, 87
Internet of Things (IoT) security, 83
iOS devices, 96
ISACs (Industry Sharing and Analysis Centers), 162
ISO 27001, 87
IT (information technology) departments, 185

J

joint partnerships, 73
just-in-time training, 184

K

keystroke sniffing, 81
knowledge metrics, 112–113
knowledgebase, 95–96

L

Landewe, Michael, 16–17
landing pages, 182, 200–201
language, 193–194
law enforcement agencies, 104
lawsuits, 110. *See also* compliance requirements
learning management system (LMS), 111–112
legal departments
  approvals, 146–147
  budget/funding, 13
  interviewing, 68, 247–248, 249
  phishing simulations, 185
LGPD, 87
lights, 83
likability metrics, 112, 149
LinkedIn, 86
LMS (learning management system), 111–112
lock picking, 1
logistics, 144–146
  phishing simulations, 201–203
  reporting, 149–153
  scheduling, 145
  sources/vendors, 144–145
logos, 140
losses
  measuring, 12–13
  NSA example, 11–12
  phishing attack, 8–11
  small, 47
  user-initiated, 10–11, 14–15

lost devices, 47
lures, 182, 187
  constructing, 197–198
  ideas, 198–199
  sophistication level, 196–197
lying, 80

M

machine learning, 192
malicious websites, 9–10
malware
  antimalware software, 29–30
  as program topic, 79, 81, 224
  ransomware, 9, 79, 81–82, 224
  USB-chargeable items, 81–83
  Wannacry, 162, 225
managed services, 192, 197, 199
management reporting, 206
management support. *See* support, winning
marketing campaigns, 24–26
mascots, 140–141
McGonigal, Jane, 167
memorable presentations, 45
mental models, 27–28
messages, 49, 182
messaging partnerships, 73
metrics, 4, 107–108
  adjusting, 154–155, 159–160
  behavioral
    gamification, 115–116
    incidents, 113–114
    overview, 113, 156–157
    simulations, 114–116, 183–184
  biasing, 139
  budget/funding, 12–13, 59, 110
  choosing, 137–139
  compliance requirements, 109–110
  Day 0 metrics, 29, 118, 138
  engagement, 111–113, 138
  hidden costs, 108–109
  lawsuits, 110
  meaningful reports, 149–153
  not collecting, 29
  periodic updates, 138–139
  phishing simulations, 57, 183–184, 204–205
  ROI, 116–117
  in strategy planning, 54, 57–58
  tracking intangible benefits, 117
  vendor tools, 108, 144–145
MFA (multifactor authentication), 9, 49, 82, 114, 174
Microsoft Exchange Server hacks, 199
mission statements, 220
mobile device security
  executive awareness program, 131
  gamification, 174
  knowledgebase, 96
  messaging security, 80
  as program topic, 84, 222
monetary rewards, 177, 218, 219
monitor displays, 89, 97–98
motivation
  B:MAP model, 42–44
  to do work right, 77–79
  in risk formula, 47
mousepads, 100, 177
moving security, 86–87
multifactor authentication (MFA), 9, 49, 82, 114, 174
multiple awareness programs, 127–129, 136, 158–159
must-do tasks
  accounting practices, 37–39
  compliance as a should-do task, 21–23
  motivating users to do thing right, 77–79

N

National Security Agency (NSA), 11–12, 84
natural disasters, 48, 49
negative consequences, 41–42, 43–44
Netflix, 86
neutral consequences, 41–42
newsletters
  as communication tool, 97
  quarterly delivery schedule, 133–136
  in strategy planning, 54, 55

non-human-related occurrences, 48
nonresilient power sources, 48, 49
North Korea, 8, 162
notebooks, 100–101
NSA (National Security Agency), 11–12, 84
nudges, 42–44, 45, 93, 224

O

Office of Personnel Management (OPM), 9
one-size-fits-most strategy, 40, 46. *See also* group psychology
operational vulnerabilities, 46–47, 49
organizational behaviors, 33
  accounting practices, 37–39
  awareness ABCs, 39–40
  common knowledge/sense, 34–35
  group psychology
    behavioral science ABCs, 41–42, 166–167
    B:MAP model, 42–44
    Fogg Behavior Model, 42–43
    Forgetting Curve, 44–45
    overview, 40
  risk management
    optimizing risk, 46
    overview, 45–46
    risk formula, 46–50
  safety science, 35–37
organizational countermeasures
  for "gaming the system," 14
  purpose, 169
  in risk formula, 46–47, 49–50
organizational culture, 61–64
  all employees, 247–248
  business drivers, 55–56, 65–66
  communications tools, 54, 55–56, 62–63
  HR departments, 249
  interdepartmental partnering, 72–73
  interviewing stakeholders
    contact information, 72
    general questions, 71
    interview content, 70–72
    overview, 67
    scheduling, 70
    whom to interview, 67–70
  metrics, 57–59, 138–139
  physical security managers, 250–251
  sample interview questions
    all employees, 247–248
    CISO/similar position, 234–247
    communications department, 250
    HR departments, 68, 249
    legal departments, 68, 247–248, 249
    overview, 233–234
    physical security managers, 250–251
  security culture versus, 55, 62, 64–65
  subcultures, 127–129, 136, 158–159
  tracking intangible benefits, 117
organizational psychology, 23–24
outside speakers, 104–105
outsourcing specialists, 126

P

pamphlets, 98
partnering, 72–73
passive communication tools, 92–93, 95
  adjusting, 155–156, 159–160
  camera covers, 101
  coffee cups, 99–100
  design styles, 93
  desk drops, 72, 99, 171–172
  engagement metrics, 111–112
  monitor displays, 89, 97–98, 100
  mousepads, 100
  other giveaways, 100–101, 177, 218, 219
  pamphlets, 98
  pens, 100–101
  printed newsletters, 54, 55, 97
  quarterly delivery schedule, 133–136
  screen savers, 98
  sleeves, 99–100
  squishy toys, 101
  stickers, 100
  table tents, 99, 133–136

password sniffing, 81
passwords, 9
  awareness ABCs, 39–40
  as awareness topic, 82, 223
  common knowledge/sense, 34
  observing user behaviors with, 114
  in risk formula, 47
  strength, 162, 167
Payment Card Industry Data Security Standard (PCI DSS), 87, 110
peer pressure, 42–44
penetration tests, 1, 34–35
pens, 100–101, 218, 219
People-Centric Security (Hayden), 230
personal awareness, 76–77
personality types, 23–26
personally identifiable information (PII), 222
personnel countermeasures, 50
personnel vulnerabilities, 46–47, 48–49
phishing attacks, 8–11, 26
  during COVID-19 pandemic, 162–164
  email messages, 14
  losses from, 8–11
  malware, 81
  as program topic, 79–80, 162, 221–222
phishing domains, 194
phishing mitigation services, 192, 197, 199
phishing simulations, 4, 29, 114–116
  adapting for metrics collection, 148
  anticipating user responses, 203
  budget/funding, 122, 125, 136–137
  caution, 131, 191, 199–200
  CBT, 189–190
  cheating, 198
  dealing with repeat offenders, 205
  ethical considerations, 131, 191, 199–200
  free alternatives, 137
  frequency, 201
  gamification, 201–202
  goals, 183–185
  GoDaddy example, 147, 191, 200
  identifying trends, 204–205
  implementing, 192–195
  lack of standards, 21
  landing pages, 182, 200–201
  logistics, 201–203
  lures
    constructing, 197–198
    ideas, 198–199
    overview, 182, 187
    sophistication level, 196–197
  management support, 186
  messages, 182
  metrics, 57, 183–184, 204–205
  pilot test, 203–204
  planning, 185–187
  reporting, 170–171, 206
  running, 181, 182
  scheduling, 202–203
  service providers, 192, 197, 199
  as tactic, 53
  targets, 195–196
  tools
    custom, 187–189
    overview, 187–188
    vendors, 108, 189–192
  understanding, 182
  whitelisting, 147, 182, 201
PhishMe software, 188
physical countermeasures, 50
physical penetration tests, 34–35
physical security, 81, 224
physical security managers, 67, 185, 250–251
physical vulnerabilities, 46–47, 48–49
PII (personally identifiable information), 222
points of contact (POC) interviews, 69, 247–248
Pokémon Go gamification, 176
popular awareness theories, 23–26
positive consequences, 41–44
post mortem reviews, 37
posters
  as communication tool, 96–97
  quarterly delivery schedule, 133–136
  in strategy planning, 54
post-incident reviews, 37
pretext telephone calls, 26, 80, 114–116

pride, sense of, 174
printed newsletters
  as communication tool, 97
  quarterly delivery schedule, 133–136
  in strategy planning, 54, 55
printing partnerships, 73
probability, 46–47
products, 29–30
professional speakers bureaus, 104
program delivery scheduling, 131–132
  reinforcement, 133
  topic distribution, 133–136
project management, 146
promotions, 177
prompts, 42–44, 45, 93, 224
psychology, 40
  behavioral science versus, 23–24
  group
    behavioral science ABCs, 41–42, 166–167
    B:MAP model, 42–44
    Fogg Behavior Model, 42–43
    Forgetting Curve, 44–45
  popular awareness theories, 23–26
public charging stations, 82–83
public Wi-Fi, 84

Q

quality control, 146–147
quarterly programs, 131–132
  responsiveness, 213–214
  topic distribution, 133–136
quizzes, 112–113

R

ransomware, 9, 79, 81–82, 224
Reality Is Broken (McGonigal), 167
regulations. *See* compliance requirements
reinforcement strategies
  Forgetting Curve, 44–45
  gamification, 166–167
  quarterly programs, 133–136
reminders, 42–44, 45, 93, 224
remote access, 81
reporting, 10, 77
  logistics, 149–153
  phishing simulations, 148, 170–171, 206
  as program topic, 79
representative employees interviews, 69, 247–248
resources, 227–228
  Cybersecurity Culture Guidelines, 229
  CybSafe Research Library, 228
  How to Run a Security Awareness Program course, 231
  Human Factor Knowledge Area paper, 230
  Human Security Engineering Consortium, 231
  People-Centric Security (Hayden), 230
  RSA Conference, 229
  SASIG, 228
  Sydney Dekker work, 230
  You Can Stop Stupid (Brown), 229
responsive tools, 187, 201
return on investment (ROI)
  countermeasures, 169
  metrics for demonstrating, 116–118
  proving, 20–21
  training time, 108–109
reward programs, 58, 87, 160, 166, 218, 219. *See also* gamification program
reward tiers, 175–177
Ring cameras, 39–40
risk management, 9–10, 45–46
  goal of, 28–29
  optimizing, 46
  risk formula, 46–50
  simulations, 184
roadshows, 133–136
ROI. *See* return on investment
role-based awareness programs, 127
RSA Conference, 229

S

safecracking, 1
safety manager interviews, 69, 234–247

safety science, 35
communications tools advice, 95
recognizing incidents as system failures, 36
responding to incidents, 37
simulations, 182
Sydney Dekker work, 230
sales incentives, 166
Salesforce gamification program, 176
sample questionnaire. *See* stakeholder interviews
SASIG (Security Awareness Special Interest Group), 228
scavenger hunts, 103, 160, 218
science, 33
accounting practices, 37–39
awareness ABCs, 39–40
behavioral science ABCs, 41–42, 166–167
common knowledge/sense, 34–35
group psychology
B:MAP model, 42–44
Fogg Behavior Model, 42–43
Forgetting Curve, 44–45
overview, 40
risk management
optimizing risk, 46
overview, 45–46
risk formula, 46–50
safety, 35–37
screen savers, 98
seasonal phishing attacks, 199
security access badges. *See* badges
security ambassadors, 209–210
adding, 160
as communication tool, 90–92
winning support via, 218
security awareness programs, 1–4, 121. *See also* budget/funding
benefits, 8–11
branding, 139–141, 146–147
characteristics of good
awareness as tactic, 14–15
behavior modification, 11–13, 14
goals, 12–13
common topics
basic computer security, 80, 81, 85, 131, 223
cloud security, 82
compliance topics, 87
insider threats, 85
instant message security, 80
IoT security, 83
malware, 81–82
mobile device security, 84
moving security, 86–87
overview, 79
password strength, 82
phishing, 79–80
physical security, 81
protecting children on the internet, 85
ransomware, 81–82
social engineering, 79, 80, 162
social media security, 86
text message security, 80
travel security, 83
USB device security, 8, 81–83, 173
Wi-Fi security, 84
work-from-home security, 76, 84
coordinating with other departments, 124–125
defining success, 39–40
executive awareness program, 131
fundamental topics
business email compromise, 222
home network security, 131, 223
incident occurrence, 225
malware/ransomware, 224
mobile device security, 222
password strength, 223
phishing attacks, 79–80, 162, 221–222
physical security, 224
social engineering, 225
social media security, 223–224
geographic considerations, 66
hidden costs, 94, 101–102, 108–109
human firewall myth, 16–17, 122, 210
NSA example, 11–12
quarterly delivery strategy

overview, 131–132
reinforcement, 133
responsiveness, 213–214
topic distribution, 133–136
resources
Cybersecurity Culture Guidelines, 229
CybSafe, 228
How to Run a Security Awareness Program course, 231
Human Factor Knowledge Area paper, 230
Human Security Engineering Consortium, 231
overview, 227–228
People-Centric Security (Hayden), 230
RSA Conference, 229
SASIG, 228
Sydney Dekker, 230
You Can Stop Stupid (Brown), 229
ROI
countermeasures, 169
metrics for demonstrating, 116–118
proving, 20–21
training time, 108–109
role of awareness, 7, 15–16, 31
running
approvals, 146–147
breaking news/incidents as topics, 161–162
COVID-19 impact, 162–164
Day 0 metrics, 147–148
enhancements, 157–161
logistics, 144–146
multiple awareness programs, 127–129, 136, 158–159
overview, 143–144
reevaluating program, 153–157
reporting, 149–153
things to avoid
addressing ineffective mental models, 27–28
Check the Box mentality, 20–21
choosing substance over style, 30–31
compliance as a should-do task, 21–23
limiting popular awareness theories, 23–26
not collecting metrics, 29
overview, 19–20
prioritizing program over product, 29–30
social engineering vs. security awareness, 26–27
unrealistic goals, 28–29
winning support for
addressing business concerns, 211, 217
being responsive, 213–214
caution with FUD factor, 218–219
establishing credibility, 213, 219
executive awareness program, 211, 215–216
finding problems to solve, 212
highlighting actual incidents, 213
hosting engaging events, 217, 218
influencers, 216
management support, 122, 129–131
mission statement integration, 220
overview, 209
security ambassadors, 90–92, 160, 209–210
setting realistic expectations, 210, 217
starting small, 212
supporting similar projects, 214, 216–217
using real gamification, 218, 219
Security Awareness Special Interest Group (SASIG), 228
security cubicles, 103
security culture
awareness ABCs, 39–40
consequences, 42
determining, 64–65
group psychology
behavioral science ABCs, 41–42, 166–167
B:MAP model, 42–44
Fogg Behavior Model, 42–43
Forgetting Curve, 44–45
overview, 40
organizational culture versus, 55, 62, 64–65
in strategy planning, 54
tracking intangible benefits, 117
security-related behavior modification
goal of security awareness programs, 11–13, 14
motivating users to do thing right, 77–79
security as a must-do task, 21–23
tracking, 113–116
senior management support, 122, 129–131
SET (Social Engineering Toolkit), 189

should-do tasks, 21–23. *See also* must-do tasks
shoulder surfing, 26
significance of information, 45
simulations, 114–116, 183–184. *See also* phishing simulations
single awareness programs, 65–66
  expanding, 158–159
  multiple versus, 127–129
SITA data breach, 213
Six Sigma-like methodologies, 117, 151
sleeves, 99–100
slogans, 140
small losses, 47
smishing, 80
Snowden, Edward, 48
social engineering, 1. *See also specific forms of social engineering*
  awareness versus, 26–27
  common knowledge/sense, 34–35
  as program topic, 79, 80, 162, 225
Social Engineering Toolkit (SET), 189
social media security, 82, 86, 223–224
software. *See specific software programs*
SolarWinds Orion, 199
Sony, 8, 117
spam bots, 81
spam filters, 201
speakers, 104–105, 160, 218
spearphishing, 79
specialists, outsourcing, 126
spoofing, 84, 194
squishy toys
  as communication tool, 101
  gamification rewards, 177
  mascots, 140–141
  support via real gamification, 218, 219
staff considerations, 126
stakeholder interviews, 67
  contact information, 72
  general questions, 71
  intangible benefits, 117
  interview content, 70–72
  sample interview questions
    all employees, 247–248
    CISO/similar position, 234–247
    communications department, 250
    HR departments, 68, 249
    legal departments, 68, 247–248, 249
    physical security managers, 250–251
  scheduling, 70
  whom to interview, 67–70
stickers, 100–101, 177
strategy planning
  budget/funding, 58–59
  business drivers in, 54, 61, 65
  components
    effective communications tools, 54, 55–56
    gamification, 54, 58
    metrics, 57–58
    overview, 54–55
    topics based on business drivers, 56–57, 76
  tactics versus, 14–15, 53–54
subcultures
  business drivers, 55–56, 65–66
  multiple awareness programs
    expanding, 158–159
    overview, 127–129, 136
  phishing simulations, 193–194
support, winning, 209
  addressing business concerns, 211, 217
  being responsive, 213–214
  caution with FUD factor, 218–219
  establishing credibility, 213, 219
  executive awareness program, 211, 215–216
  finding problems to solve, 212
  highlighting actual incidents, 213
  hosting engaging events, 217, 218
  influencers, 216
  mission statement integration, 220
  security ambassadors
    adding, 160
    as communication tool, 90–92
    overview, 209–210
  setting realistic expectations, 210, 217
  starting small, 212
  supporting similar projects, 214, 216–217
  using real gamification, 218, 219

sustainability team, 69, 247–248
system failures, 35
  common causes of
    Check the Box mentality, 20–21
    choosing substance over style, 30–31
    ineffective mental models, 27–28
    not collecting metrics, 29
    overview, 19–20
    phishing attacks, 15–16
    popular awareness theories, 23–26
    prioritizing program over product, 29–30
    should-do compliance, 21–23
    social engineering vs. security awareness, 26–27
    unrealistic goals, 28–29
  human firewall myth, 16–17, 122, 210
  recognizing incidents as, 36
  responding to, 37
  user-initiated loss, 10–11

T

table tents, 99, 133–136
tactics, 14–15, 53–54
tailgating, 80, 81, 148, 172–173
tangible benefits, 108–109. *See also* return on investment
Target, 8, 117
tchotchkes, 177
technical countermeasures, 49
technical tools, 44, 49
technical vulnerabilities, 46–47, 48–49
telephone pretext calling, 26, 80, 114–116
terrorists, 24, 49
text messaging security, 80
theft, 34–35, 77, 80
third-party compliance requirements, 20–21
  CBT, 102
  mandated tools, 125
  metrics, 109–110
  phishing simulations and, 183
threat, 46–48
thumb drives, 81–83, 173
TikTok, 86
Tiny Habits (Fogg), 42
tools, 89–90. *See also* communications tools
  engagement metrics, 111–112
  gamification, 179
  phishing simulations
    custom tools, 188–189
    overview, 187–188
    vendor tools, 108, 189–192
  quarterly delivery schedule, 133–136
  technical, 44, 49
topics, 75
  based on business drivers, 56–67, 76
  breaking news/incidents, 161–162
  common
    basic computer security, 80, 81, 85, 131
    cloud security, 82
    compliance topics, 87
    insider threats, 85
    IoT security, 83
    malware, 81–82
    messaging security, 80
    mobile device security, 84
    moving security, 86–87
    overview, 79
    password strength, 82
    phishing, 79–80
    physical security, 81
    protecting children on the internet, 85
    ransomware, 81–82
    social engineering, 79, 80, 162
    social media security, 86
    travel security, 83
    USB device security, 81–83
    Wi-Fi security, 84
    work-from-home security, 76, 84
  distributing over three months, 133–137
  Forgetting Curve, 133–136
  fundamental
    business email compromise, 222
    home network and computer security, 131, 223
    incident occurrence, 225
    malware/ransomware, 224
    mobile device security, 222

topics *(continued)*
  password strength, 223
  phishing attacks, 221–222
  physical security, 224
  social engineering, 225
  social media security, 223–224
 important to individuals, 216
 motivating users to do thing right, 77–79
 personal awareness, 76–77
 reusing, 160–161
 in strategy planning, 54, 56–57
toys
 as communication tool, 101
 gamification, 177, 218, 219
 mascots, 140–141
training teams
 hidden costs, 108–109
 interviewing, 68, 247–248
 just-in-time training, 184
 motivating users to do thing right, 77–79
training videos, 54, 93, 230
transactional influence, 27
travel security, 83
triggers, 199–200
T-shirts, 177, 218, 219
Twitter, 49, 76, 86, 162

U

Understanding Human Error video series, 230
uninterruptible power supplies, 48, 49
unions, 68, 247–248
University of Bristol CyBOK project, 230
unpredictable attacks, 76
unsecured computers, 80, 81, 85
USB devices, 8, 81–83, 173
user experience, 36
users
 authentication security checks, 21
 awareness, 8–11
 identifying risky vs. secure, 184
 losses initiated by, 10–11, 14–15
 MFA, 9, 49, 82, 114, 174
 in risk formula, 47

V

value, 46–47
vendor tools, 108
 logistics, 144–145
 phishing service providers, 197, 199
 phishing simulations, 189–192
Verizon Data Breach Investigations Report (DBIR), 3, 9, 85
videos, 54, 93, 230
voice phishing (vishing) attacks, 76, 162
VPN software, 84
vulnerabilities, 46–47, 48–49

W

Walmart, 65–66
Wannacry malware, 162, 225
web browsing, 81, 114
well-meaning users, 47–48
wellness programs
 communications tools advice, 95
 interviewing, 68–69, 247–248
 support for awareness programs, 214
whaling attacks, 79
whitelisting, 147, 182, 201
Wi-Fi networks, 8, 84, 96, 131, 223
wikis, 95–96
work-from-home (WFH) security, 76, 83–84
 COVID-19 impact, 162–164
workplace injuries, 35
 increased funding due to, 47
 as program topic, 161–162, 225
 recognizing as system failures, 36
 report gamification, 173
 responding to, 37
 in strategy planning, 54
worm-like attacks, 81

Y

You Can Stop Stupid (Brown), 10, 47, 229
YouTube, 229, 230