

INDEX

A

accessibility requirements, 39
active exploitation, 120
advantages of tabletop exercises, 13–14
 efficiency, 14
 high return on investment, 13
 low cost, 13
 no operational disruption, 14
Amazon, 16
attendees, 38–40. *See also* participants
 tasks, 93–94
audiovisual needs, 39
auditors, 48

B

backchannels, 96–97
board of directors, 9
breakout groups, 93–94
breakout rooms, 91
budget, information security, 17–18
business continuity plan, 19
business-focused tabletop exercises,
 145–155
 insider threat example, 152–154
 physical security breach example,
 145–148
 social media compromise example,
 148–152
business impact analysis, 52

C

Calce, Michael, 16
calendar invitations, 43
case studies
 ad hoc response to current
 events, 17
 far-fetched scenario, 54–55
 fostering security awareness, 8–9

 media training, 92–93
 relevant scenario, 56
 responding to new laws, 6
 scenario exploring organizational
 weaknesses, 57
 testing manufacturing systems, 15
 vendor-focused exercise, 31–32
casino hacks, 16
Center for Internet Security (CIS),
 10, 11
charter for incident response plan, 19
chief information security officer
 (CISO), 5, 6, 39, 99
CISA (Cybersecurity and
 Infrastructure Security
 Agency), 13–14, 58
co-facilitator, 86, 92
collaboration on the incident response
 team, 4
Colonial Pipeline, 16, 17
communication lead, 42, 43
communication processes,
 evaluating, 28
communications and marketing
 firms, 30
communication tips, 96–101
 checking in with senior
 attendees, 97
 considering the question structure,
 99–100
 forging interpersonal connections,
 98–99
 identifying sensitive topics in
 advance, 101
 managing conversation hogs, 97–98
 monitoring physiological
 responses, 96
 paying attention to nonverbal
 communication, 100

- communication tips (*continued*)
 - practicing cultural awareness, 100–101
 - setting up backchannels, 96–97
- Computer Security Incident Handling Guide* (NIST SP 800-61r2), 19, 111
- conference rooms, 38–39, 94–95
- confidentiality, 45–46
- confirmed compromises, 20
- containment procedures, 14, 19
- contracts, 11
- conversation hogs, managing, 97–98
- Cost of a Data Breach* (Ponemon Institute and IBM Security), 7, 14
- COVID-19 pandemic, 17
- credit cards, 11
- cross-training, 47
- cryptocurrency mining, 15
- cultural awareness, 100–101
- cyber insurance, 48, 58, 113–114
- Cybersecurity and Infrastructure Security Agency, 13–14, 58
- cybersecurity tabletop exercises, xix

D

- dark web data discovery example, 138–141
- data breaches, 7
 - confirmed vs. suspected, 20
 - financial impact of, 6–7
 - notification requirements, 20–21
 - temporal requirements, 20
- Data Protection Act, 6
- date and time, choosing, 37–38
- DDoS attacks, 16, 141–143
- debrief, performing, 105–106
- Defense Federal Acquisition Regulation Supplement (DFARS), 10, 11
- Department of Health and Human Services, 20
- Department of Homeland Security, xxii
- development lead, 33–34
- development team, 33–36, 43–44, 103–104, 107, 112, 113
 - evaluator, 36
 - facilitator, 34

- lead, 33–34
- observer, 35
- subject matter expert, 34–35
- trusted agent, 35
- discussion session, 43–44
- distributed denial-of-service (DDoS) attacks, 16, 141–143
- documentation, cataloging and updating, 112
- DoD (Department of Defense), 11
- duration, determining, 37

E

- eBay, 16
- email notification, 42–43
- encouraging participation, 76–77
- ENISA (European Union Agency for Cybersecurity), 14, 16, 110
- escalation of threats, 8
- escalation pace, scenario, 67–68
- ethical responsibility, 21
- etiquette for tabletop exercise, 75
- European Union Agency for Cybersecurity, 14, 16, 110
- evaluation methods, 105–107
 - performing a debrief, 105
 - sending a survey, 106–107
- evaluation requirements, 103–104
- evaluation restrictions, 104
- evaluator, choosing an, 104–105
- examining a recent cybersecurity incident, 12
- executive audience, 135
- executive checkpoint, 41–42
- executive sponsor, 24, 41–43, 53, 96, 101, 105, 107, 108, 113–114
 - responsibilities for, 25–26
 - selecting, 24
- executive tabletop exercises, 9, 135
 - dark web data discovery example, 138–141
 - DDoS attack example, 141–143
 - ransomware example, 136–138
- external facilitator, 47
- external party notifications, 19
- external sites, 39–40
- external stakeholders, 48, 113
- external vendors, 30

F

- facilitator, 83–85
 - challenging attendees, 84
 - creating an adversarial environment, 85
 - external, 47
 - leading the witness, 84
- facilitator space, 39
- facility, securing, 38
- feedback, inviting, 80
- final reminder, 44–45
- financial impact of data breaches, 8
- findings, 108–109, 114
- focus areas, 15
 - budget, 17–18
 - efficacy of processes and procedures, 19
 - incident response plans, 19
 - information sharing protocols, 18
 - notification compliance, 20–21
 - residual risk, 21
 - threat landscape, 16
- follow-up activities, 111–114
 - assessing the incident response plan, 112
 - cataloging and updating documentation, 112
 - communicating exercise findings, 114
 - conducting further tabletops, 113
 - identifying and analyzing trends, 114
 - implementing a formal tabletop exercise program, 113–114
- formal tabletop exercise program, implementing, 113–114
- “A Framework for Cybersecurity Information Sharing and Risk Reduction” (Microsoft), 18
- frameworks, compliance with, 10
- French National Agency for the Security of Information Systems, xxii
- full report, 108, 159
 - findings and observations, 108–109
 - recommendations, 109

- sample, 110–111
- template, 159–164

G

- General Data Protection Regulation (GDPR), 20
- goals and objectives, 26–28, 77
- ground truth document, 68–73
 - aligning with objectives, 70
 - details and expected outcomes, 69–70
 - example, 70–73
 - maintaining realism, 70
- Guardians of Peace, 16
- guest presenter, 86

H

- hands-on exercises vs. tabletop exercises, 13
- Health Insurance Portability and Accountability Act (HIPAA), 20
- Homeland Security Exercise and Evaluation Program (HSEEP), xxii, 68
- human resources manager, 5

I

- IBM Security, 7, 14
- impact, assessing, 5–6, 109
- incident escalation paths, 19
- incident identification and notification, 19
- incident response lifecycle, 64
- incident response plans, 27, 30, 112
 - charter, 19
 - deficiencies in, 15, 19
 - rehearsing, 27
 - team roles and responsibilities, 19
 - testing, 7
- indicators of compromise, 18
- industry peers, 59
- industry standards, aligning with, 10–11
- informal touchpoints, 44
- information security budget, 17–18
- information security manager, 5
- information sharing protocols, 18

- injects, 78
 - clarity and conciseness, 63
 - date and time, 79
 - defined, 59
 - directing focus, 62
 - executive, 60
 - imagery, 79
 - media, 62
 - nontechnical, 61
 - simulating time constraints, 61
 - technical, 60
- in-person exercises, 36–37
- insider threat example, 152
- intended outcomes, 77–78
- International Organization for Standardization (ISO), xxii, 10
- interpersonal connections, 98–99
- The Interview* (film), 16
- IoC (indicator of compromise), 18
- ISO/IEC 27001, 10

K

- Kim Jong Un, 16
- known risks, identifying and prioritizing, 12

L

- lateral movement, 52
- law enforcement, 58
- laws, responding to, 6
- legal privilege, 32
- legal support, 5, 32–33, 107
- lessons learned
 - from incident response, 12
 - from tabletop exercises, 13
- logistical considerations, 36–41, 43
 - date and time, 37–38
 - duration of exercise, 37
 - remote vs. in-person exercises, 36–37
 - securing a facility, 38–40
 - setting the tone, 40–41

M

- malicious software, 15
- malware outbreak example, 126–130

- managed security services provider (MSSP), 27–28, 30
- management tasks, 85–87
 - adding a co-facilitator, 86
 - assigning a scribe, 85
 - inviting a guest presenter, 86
 - prewriting questions, 87
- manufacturing systems, 15
- Microsoft, 18
- mission statement in incident response plan, 19
- moral responsibility, 21
- Morris, Robert, 16
- Morris Worm, 16
- multimedia aids, 92

N

- National Institute of Standards and Technology (NIST), xxii, 10, 64
 - incident response lifecycle, 64
 - SP 800-3, 110
 - SP 800-61r2, 19, 111
 - SP 800-84, 10, 106
 - SP 800-171, 11
- network administrator, 5
- North Korea, 16
- nonverbal communication, 100
- Nonverbal Communication* (Burgoon, Manusov, and Guerrero), 100
- notifications, 41
 - calendar invitations, 43
 - discussion session, 43–44
 - email, 42–43
 - executive checkpoint and, 41–42
 - external party, 19
 - final reminder, 44–45
 - informal touchpoints, 44
 - requirements, 20–21

O

- objectives vs. goals, 26–27
- observations, 108–109
- observer, 35
- operational-level exercises, 28–29
- opposition from invitees, 46–47
- organizational culture, 37
- outsourcing tabletop exercises, 47–48

P

- participants
 - accessibility requirements, 39
 - convenience for, 38–39
 - determining, 29–30
 - notifying, 41–43
 - number of, 39
 - opposition from, 46–47
 - social distancing, 39
- Payment Card Industry Data Security Standard (PCI-DSS), 11
- penetration testing, 15
- personal data, 6
- phishing, 8–9, 120–123
- physical security breach example, 145–148
- physiological responses, 96
- playbooks, 19
- polling software, 88–89
- Ponemon Institute, 7, 14
- presentation deck, 73–80
 - debrief, 80
 - injects, 78–80
 - introductions, 74
 - preamble, 74–78
- prewritten questions, 79–80, 87
- printing and mailing firms, 30
- priority of stakeholders, 39
- process changes, assessing impact of, 5–6
- processes, updating, 112
- processes and procedures, efficacy of, 19

Q

- question structure, 99–100

R

- ransomware, 13, 16, 56, 57
 - examples
 - executive exercise, 136–138
 - technical exercise, 123–126
- rationale for tabletop exercise, 75
- realism
 - in ground truth document, 70
 - of scenario, 54–55
- reasons to conduct tabletop exercises
 - align with industry standards, 10–11

- assess impact of process changes, 5–6
- clarify team roles and responsibilities, 4–5
- examine a recent cybersecurity incident, 12
- explore key questions, 9
- fulfill contractual requirements, 11
- identify and prioritize known risks, 12
- improve relationships, 4
- improve security awareness, 8–9
- prepare senior leadership for incidents, 9–10
- reduce the cost of data breaches, 6–7
- recommendations based on findings and observations, 109
- recording devices and software, 94
- red teams, 7, 13
- relevant scenarios, 55
- remote exercises, 36–37
- remote presentation software, 91–92
- reporting conventions, 107–111
 - full report, 108–110, 159–164
 - statement of completion, 107–108, 157–159
- requirements and restrictions, 103–104
- residual risk after corrective action, 21
- responsibilities of team, 4–5
- return on investment, 13
- risk disclosures, 10
- risk management, 5
- risk register, 12

S

- sample report, 110–111
- Saudi Arabia, 16
- Saudi Aramco, 16
- scenarios, 53
 - characteristics of effective, 53–57
 - inspiration for, 57–59
- scribe, 85, 92, 108
- SEC (Securities and Exchange Commission), 9–10, 59
 - Form 8-K, 20
 - Form 10-K, 9–10, 59
- security awareness, 8–9

- security incidents, preparing senior leadership for, 9–10
- security operations center (SOC), 30, 47
- senior attendees, 97
- senior-level exercises, 28–29
- sensitive topics, 101
- Shamoon virus, 16
- smishing, 17
- social distancing, 39
- social media, 13
- social media compromise example, 148–152
- Sony Pictures, 16
- stakeholders, 4, 39
- statement of completion, 107–108
 - template, 157–159
- storyboard
 - designing, 63–67
 - examples, 65, 69
- Stuxnet, 16
- subject matter expert, 34–35
- supply chain attack, 130
- supply chain compromise example, 130–133
- surveys, sending, 106–107
- suspected compromises, 20

T

- tabletop exercises. *See also* advantages of tabletop exercises; focus areas; logistical considerations
 - defined, 3
 - educational component, 74
- tactics for tabletop exercises, 88, 93–94
- tandem exercises, 29
- team responsibilities, 4
- technical audience, 119
- technical tabletop exercises, 9, 119
 - malware outbreak example, 126–130
 - phishing campaign example, 120–123
 - ransomware example, 123–126
 - supply chain compromise example, 130–133

- testing frequency, 19
- third-party assessment, 48
- threat landscape, 16
- threats, identifying, 8
- tools for tabletop exercises, 88
 - multimedia aids, 92–93
 - polling software, 88–91
 - recording devices and software, 94
 - remote presentation software, 91–92
 - writing board, 88
- tone, setting the, 40–41
- topic, choosing a, 52–53
 - conferring with executive sponsor, 53
 - consulting business impact analysis, 52
 - leveraging other resources, 53
- trend analysis, 114
- trusted agent, 35, 96–97

U

- US Department of Defense (DoD), 11
- US Department of Health and Human Services, 20
- US Department of Homeland Security, xxii
- US Securities and Exchange Commission (SEC), 9–10, 20, 59

V

- vCISO (virtual chief information security officer), 30, 47
- vendor response, assessing, 27–28
- vendors, working with, 30–32

W

- working the room, 95–96
- writing board, 88

Y

- Yahoo, 16