

## A

A. P. Møller - Maersk, xxv

Accept option, in risk response, 180

access control lists (ACLs), 238

account usage artifacts, 224

accountability, 275

Accountable, in RACI chart, 159

accuracy, of data, 190, 270, 275

Acquire Additional Data step, in analysis lifecycle, 201–202

acquisition method, 199

Act step, in Deming cycle, 185

actionable intelligence, 175, 235–236

active voice, writing in, 222

admissibility, of digital evidence, 258–265

advanced persistent threats (APTs), 2–3

advanced static analysis, 217

adversary. *See* threat actors

adverse event, 9

agent-based collection,

134–135

agentless collection,

134–135

alerting the attacker,

236–237

alerts, 9–10, 132

Align TTPs to Target phase, of cyberattack preparation framework, 6

Altaba, 248

Amazon Web Services (AWS), 116, 117, 119

analysis

automating tasks, 101

in incident response  
playbook workflow,  
174–175

performing, 200–222

processing data before,  
100

of requirements, 34

Analysis/Analyze phase

in EDRM, 254, 256–257

in lessons-learned

process, 181–182

Analyze Data step, in

analysis lifecycle,

200–201

Analyze Information

step, in seven-step

improvement process,

187, 191

antivirus software,

128–129

application group, 88

application logs, 130–131

architectures, for log

management, 135–137

artifacts, 223

Assess Findings and Create

Plan step, in seven-step  
improvement process,  
187, 191–192

assessing readiness,  
235–236

Assessment step, in  
strategic planning,  
23–24

asset management, 156

assigning roles and  
responsibilities, 82–90

atomic indicators, 213

attack vector, 209–210

attacker. *See* threat actors

attorney work-product,  
264

attorney-client privilege, 86,  
263–264

attribution, cyber, 248–250

audience, knowing your,  
222

audit events, 131

audit logs, 126

auditability, of data, 270

authenticity, Federal Rules  
of Evidence (FRE) and,  
259

authority, establishing,  
75–77

automating, 100, 101

availability, of data, 189–190

Avoid option, in risk

response, 180

AWS VPC flow logs, 119

**B**

backdoor malware, 215  
 Bash shell, 110  
 basic static analysis, 216  
 Behavioral Characteristics, CTI and, 210  
 behavioral indicators, 213  
 behavioral questions, 73  
 bespoke malware, 216  
 best evidence rule, 262–263  
 Bianco, David, 211  
 breaches, 11–12. *See also* cyber breach response  
 British Airways, 22  
 browsing history artifacts, 224  
 budget, for remediation planning, 234  
 business alignment, 44  
 business case, developing, 35–37  
 business continuity and disaster recovery (BCDR), 18, 157–158  
 business process tier, for risk management, 14  
 business records exception rule, 262  
 businesses  
   changing objectives, 22–23  
   incident response teams and functions of, 82–85  
   recovering operations of, 149  
   remediation planning considerations, 233–234  
   remediation planning partners, 233–234

**C**

C2 communication, 228  
 Cancelled state, for incidents, 168  
 capabilities, 155  
 Capability Maturity Model Integration (CMMI), 30–31, 153  
 Carbon Black, 110–111  
 categorizing indicators, 212–214  
 Center for Research and Evidence on Security Threats' (CREST) Cyber Security Incident Response Maturity

  Assessment maturity model, 30  
 centralized log management architecture, 135, 136  
 centralized team model, 63–64  
 CERT Coordination Center (CERT/CC), 52  
 chain of custody  
   about, 265–266  
   defensible protocol, 266  
   establishing, 265–271  
   traditional forensic acquisition, 267–268  
 change management, 157  
 Check step, in Deming cycle, 185  
 chief information security officer (CISO), as key stakeholder, 43  
 circumstantial evidence, 260–261  
 CIS Critical Security Controls, 37  
 classifying malware, 214–216  
 client connection logs, 126  
 clipboard contents artifacts, 226  
 cloning, 104  
 closed source freeware, 99  
 Closed state, for incidents, 168  
 cloud computing, 113, 115–118  
 cloud computing forensics, 205  
 Collect Data step, in seven-step improvement process, 187, 189–190  
 Collection and Storage phase, in log management lifecycle, 133–137  
 collection methods, 252–258, 270–271  
 Collection phase  
   in CTI lifecycle, 208–209  
   in EDRM, 254, 255  
 command center, 170  
 commercial tools, 98–99  
 commodity malware, 215  
 common point of purchase (CPP), 158  
 communication flow, 80–82  
 communications  
   in incident response playbook workflow, 177  
   managing, 94  
   for remediation planning, 233, 235  
 competencies, 55, 68  
 competency model, 68–69  
 completeness, of data, 190  
 compliance  
   considerations for, 20–21  
   data privacy management and, 158  
   incident response teams and functions of, 86  
   role of, 86  
 comprehensive analysis, forensic acquisition and, 107  
 computed indicators, 213  
 Computer Emergency Response Team (CERT), 51  
 computer forensics, 203–204  
 Computer Fraud and Abuse Act (CFAA), 245  
 confidentiality policy, 42, 275  
 configuration management, 156  
 consent, 275  
 console, 110  
 Consulted, in RACI chart, 159  
 Contain Incident step, in remediation workflow, 229–230  
 Containment, Eradication, & Recovery phase  
   about, 202  
   of incident response lifecycle, 147–149  
   in incident response playbook workflow, 176  
   remediation and, 238–240  
 continual improvement  
   about, 27, 184  
   governance and, 44–46  
   in Preparation phase of incident response lifecycle, 145  
   principles of, 184–186  
   seven-step improvement process, 187–192  
 contracts, 275, 276  
 control, as risk component, 17  
 Control Objectives for Information and Related Technology (COBIT) 5, 13–14

- converting data, 191
- Coordinated Universal Time (UTC), 206
- core competencies, 68
- Corporate Communications department, incident response teams and, 83
- Corporate Security department, incident response teams and, 83–84
- Correlation and Analysis, in log management lifecycle, 133–134
- correlation rules, 139
- Cost of a Data Breach Study, xxv–xxvi
- costs, 36, 92–93
- CPP notification, 162
- crisis committee, 90
- CrowdStrike Falcon, 110–111
- CSIRT coordinational model, 78–82
- culture, impact on cyber breach response of, 44
- customization requirements, for hardware, 101
- cyber attribution, 248–250
- cyber breach response
  - about, 2, 8–9, 12
  - alerts, 9–10
  - benefits of programs, xxvi–xxvii
  - breaches, 11–12
  - compliance requirements for, 21–22
  - drivers for, 13–23
  - events, 9
  - incidents, 10–11
  - incorporating into cybersecurity programs, 23–27
  - observations, 10
  - stakeholders with interest in, 43
- cyber breaches, 11–12
- cyber insurance, 252
- cyber resilience, 17–18
- cyber risks, xxvi, 17. *See also* risks
- Cyber Security Framework (CSF), 35–37
- cyber security incident response plan (CSIRP), 38
- cyber threat intelligence (CTI)
  - about, 18–19, 60, 207
- categorizing indicators, 212–214
- as a driver for cyber breach response, 18–20
- identifying attacker activity with, 209–212
- importance of, 19–20
- lifecycle, 208–209
- malware analysis and, 217
- as a prerequisite to threat hunting, 219
- cyberattacks
  - execution framework, 4–8
  - lifecycle, 4–8
  - preparation framework, 4–7
  - risk of, 2
- cyberbullying, 4
- cybersecurity breaches, 11–12
- cybersecurity incident response team (CSIRT)
  - about, 38, 51
  - assigning roles and responsibilities, 82–90
  - building, 51–94
  - enacting, 78–82
  - history of, 52–55
  - incident response competencies and functions, 55–61
  - outsourcing partners, 90–94
  - role of in enterprises, 52–55
- cybersecurity programs
  - designing, 24–25
  - implementing components of, 25–26
  - incorporating cyber breach responses into, 23–27
  - operations, 26–27
- cyberstalking, 4
- D**
- data. *See also* personal data
  - converting, 191
  - in DIKW hierarchy, 186
  - preserving, 198–200
  - reviewing initial, 197
- Data, Information, Knowledge, Wisdom (DIKW) hierarchy, 184, 185–186
- data acquisition
  - about, 174, 198–200
  - automating, 100
  - forensic data, 102–113
  - integrating sources for, 101
  - processing before analysis, 100
- data breach, 11, 86
- data controller, 274
- data destruction, 215
- data isolation, for hardware, 102
- data loss prevention (DLP), 128
- data minimization, 275
- data of interest, identifying, 198
- data privacy, 271
- data privacy incident policy, 42
- data processing, investigations and, 274–275
- data processor, 274
- data recovery, forensic acquisition and, 107
- data retention policy, 42
- data staging, 227
- data theft, 227, 228
- databases, 126
- debug-level logging, 131
- deception technology, 129–130
- Defense Advanced Research Projects Agency (DARPA), 52
- defensible protocol, 266, 268–271
- Define a Visual for Improvement step, in seven-step improvement process, 187–188
- Define Metrics step, in seven-step improvement process, 187, 188–189
- Defined level, in CMMI, 31
- Deming cycle, 184–185
- deployment tools, 58–59
- destructive malware, 215
- Detection, in incident response playbook workflow, 173–174
- Detection and Analysis phase, of incident response lifecycle, 145–147
- Determine Purpose step, in threat hunting lifecycle, 219–220

- Develop Remediation Plan step, in remediation workflow, 229–230
  - digital asset, as risk component, 17
  - digital evidence
    - about, 252–253
    - admissibility of, 258–265
    - collecting, 252–258
    - establishing chain of custody, 265–271
    - Federal Rules of Evidence (FRE) and, 261–263
    - lifecycle, 253–258
    - litigation hold, 265
    - types of, 260–261
    - working with legal counsel, 263–265
  - digital forensics
    - about, 60, 203
    - considerations in, 206
    - disciplines, 203–205
    - timeline analysis, 205–206
  - digital forensics and incident response (DFIR), 59–60
  - direct attack, 6
  - direct evidence, 260
  - Direction stage, in CTI lifecycle, 208
  - disaster recovery, incident response teams and, 88–89
  - disaster recovery plan (DRP), 89, 149
  - disk imaging, 103–105
  - Disposal, in log management lifecycle, 133–134
  - Dissemination stage, in CTI lifecycle, 208, 209
  - distributed log management
    - architecture, 135, 136
  - distributed team model, 64–65
  - DNS flood, 124
  - DNS hijacking, 124
  - DNS tunneling, 124
  - Do step, in Deming cycle, 185
  - Document stage, in lessons-learned process, 181
  - documentary evidence, 261
  - documenting
    - about, 174
    - actions and decisions, 199
    - defensible protocol, 268–271
    - processes and procedures, in Preparation phase of incident response lifecycle, 145
    - requirements, 34, 38–39
    - roles and responsibilities, 94
  - Domain Name System (DNS), 123–125
  - dwell time, 12
  - dynamic analysis, 217
  - Dynamic Host Configuration Protocol (DHCP), 125, 204
- E**
- Elastic Block Store (EBS)
    - volume, 116
  - Elastic Compute Cloud (EC2), 116
  - Electronic Communications Privacy Act (ECPA), 245
  - Electronic Discovery Reference Model (EDRM), 253–258
  - employee investigation policy, 42
  - EnCase Forensic Software, 107
  - endpoint detection and response (EDR), 110–111, 129, 150
  - engagement process, 94
  - enterprise incident response, 196
  - enterprise security policy, 41
  - enterprise-grade tools, 110
  - Equifax, xxv
  - Eradicate Attacker step, in remediation workflow, 229–230
  - error logs, 126
  - error messages, 132
  - escalate privileges phase of cyberattack execution framework, 8
  - escalation, 174
  - escalation policy, 42
  - Establish Foothold phase, of cyberattack execution framework, 8
  - Establish Remediation Team step, in remediation workflow, 229–230
  - European Union, laws, regulations, and standards in, 246
  - European Union Agency for Cybersecurity (ENISA), 10–11
  - Evaluate stage
    - in lessons-learned process, 181–182
    - in vulnerability management lifecycle, 178–179
  - event management, 157, 161
  - events, 9
  - evidence types
    - about, 223
    - network artifacts, 226–227
    - security alerts, 227–228
    - system artifacts, 223–226
  - Execute step, in threat hunting lifecycle, 220
  - execution plans,
    - developing, 237–238
  - execution scheduling, 237
  - execution timing, for remediation planning, 233
  - executive alignment,
    - developing, 35–37
  - executive buy-in, for remediation planning, 233
  - executive leadership, as key stakeholders, 42
  - Executive level
    - of CSIRT coordinational model, 79–80
    - for incident response exercises, 57
    - metrics for, 27
    - exposure, as risk component, 17
  - external devices artifacts, 224
  - external notifications, as a source of incident notifications, 162
  - External Reconnaissance phase, of cyberattack preparation framework, 6
- F**
- facilities, for remediation planning, 235
  - facts, focusing on, 222
  - fairness, 274
  - Family Educational Rights and Privacy Act (FERPA), 21
  - Fast Flux, 124

- Federal Information Security Management Act (2002) (FISMA), 21
  - Federal Rules of Civil Procedure (FRCP), 245
  - Federal Rules of Evidence (FRE), 245, 258–259, 261–263
  - feedback loop, 5
  - Feedback stage
    - in CTI lifecycle, 208, 209
    - in threat hunting lifecycle, 220, 221
  - Fidelis Endpoint, 110–111
  - file and folder opening artifacts, 224
  - File Transfer Protocol (FTP) server, 111–112
  - filesystem artifacts, 224
  - Finance department, incident response teams and, 84–85
  - financial disclosure, materiality in, 247–248
  - financial management, 158
  - firewall logs, 118–119
  - follow the sun model, 64–65
  - food, for remediation planning, 235
  - forensic acquisition
    - about, 102–113
    - cloud computing and, 115–117
    - traditional, 267–268
  - forensic duplication, 102–108
  - forensic evidence, identifying in enterprise technology services, 123–130
  - forensic imaging, 102–108, 267
  - formal language, writing in, 222
  - formatting, of data, 191
  - frameworks, 37, 218
  - full authority model, 75–76
  - full-packet capture (PCAP), 120–122
  - functional competencies, 68
  - functional escalation, 169
  - functions, 55–61
- G**
- gap analysis, 28–30
  - gathering requirements, 33
  - General Data Protection Regulation (GDPR), 21–22, 246, 273–277
  - Generate IOCs step, in analysis lifecycle, 201
  - Generation phase, in log management lifecycle, 133–134
  - goals, 33, 210
  - Gorecki, Andrew (author), xxix
  - governance, 40–46
  - Gramm-Leach-Bliley Act (GLBA), 21
- H**
- hacktivists, 3–4
  - hard indicators, 212
  - hard skills, 69–71
  - hardware, procuring, 101–102
  - hardware write blockers, 105
  - Health Insurance Portability and Accountability Act (HIPAA), 21
  - hearsay rule, 261–262
  - helpfulness, Federal Rules of Evidence (FRE) and, 259
  - hierarchical escalations, 169
  - high-fidelity indicators, 212
  - hiring personnel, 69–75, 145
  - hold order, 265
  - honeynets, 129–130
  - honeypots, 129–130
  - horizontal communication, 63
  - Human Resources (HR) department, incident response teams and, 82–83
  - hybrid log management architecture, 137
  - hybrid team model, 65
  - hypervisor, 115, 117
  - hypotheses, establishing, 198
- I**
- IBM Cloud, 116
  - IBM X-Force Exchange, 214
  - IBM X-Force Incident Response and Intelligence Services (X-Force IRIS), 4, 5
  - identifiable natural person, 273
  - Identification phase, in EDRM, 254
  - Identify stage
    - in lessons-learned process, 181
    - in vulnerability management lifecycle, 178–179
  - imaging, 267
  - impact, 164
  - Implement stage, in lessons-learned process, 181–182
  - Implement the Plan step, in seven-step improvement process, 187, 192
  - implementation
    - of cybersecurity program components, 25–26
    - of lessons learned, 59
  - In Progress state, for incidents, 168
  - incident closure, 171
  - incident commander, 80–81
  - incident escalations, 169
  - incident information, capturing, 167–168
  - incident management
    - about, 61, 150–151
    - procedures for, 153
    - process of, 151–155
    - workflow for, 160–171
  - incident manager, 81–82
  - incident notifications, sources of, 160–162
  - incident officer, 80–81
  - incident responders, stress level for, xxiii–xxiv
  - incident response, 12, 56–57
  - incident response lifecycle
    - about, 143–144
    - Containment, Eradication, & Recovery phase, 147–149
    - Detection and Analysis phase, 145–147
    - Post-Incident Activity phase, 149–150
    - Preparation phase, 144–145
  - incident response plan
    - about, 143
    - continual improvement, 184–192
    - creating, 143–192
    - incident management, 150–160
    - incident management workflow, 160–171
    - incident response lifecycle, 143–150

- incident response
    - playbook, 171–177
    - post-incident evaluation, 177–184
  - incident response playbooks
    - about, 171–173
    - creating, 171–177
    - workflow components of, 173–177
  - incident response policy, 37–38
  - incident response team
    - about, 54
    - assigning roles and responsibilities, 82–90
    - business functions and, 82–85
    - choosing models for, 62–66
    - communication flow, 80–82
    - establishing authority, 75–77
    - hiring personnel, 69–75
    - information technology functions and, 87–89
    - introducing to enterprises, 77–78
    - legal and compliance and, 85–86
    - organizing, 66–69
    - senior management and, 89–90
    - training personnel, 69–75
  - incidents
    - about, 10–11
    - analysis of, 147
    - categorization of, 163
    - classification and documentation of, 162–168, 173–174
    - investigating (*See* investigating)
  - indicators
    - categorizing, 212–214
    - from external sources, 250
  - Indicators of Compromise (IOC), 91, 210
  - indirect attack, 6
  - indirect authority model, 76
  - industry standard assessment, 29
  - Information, in DIKW hierarchy, 186
  - Information Governance phase, in EDRM, 254
  - information stealer, 215
  - Information Systems Audit and Control Association (ISACA), 13–14
  - Information Systems tier, for risk management, 14
  - information technology functions, incident response teams and, 87–89
  - Information Technology Infrastructure Library (ITIL), 152–153
  - informational impact, 164, 165
  - informational-level logging, 131–132
  - Informed, in RACI chart, 159
  - infrastructure, 249–250
  - Infrastructure phase, of cyberattack preparation framework, 6
  - infrastructure-as-a-service (IaaS) model, 113, 114, 205
  - in-house software tools, developing, 100–101
  - Initial Compromise phase, of cyberattack execution framework, 8
  - Initial level, in CMMI, 31
  - insider threats, 3
  - integrated team, 66
  - integrity, 275
  - Intelligence Enrichment, 201, 207
  - intent, 250
  - internal investigation, forensic acquisition and, 107
  - Internal Reconnaissance phase, of cyberattack execution framework, 8
  - International Electrotechnical Commission (ISO/IEC) 27005, 13–14
  - International Organization for Standardization, 13–14
  - interviews, conducting, 73–74, 197
  - intrusion detection systems (IDS), 10, 127
  - intrusion prevention systems (IPS), 127
  - inventory, in execution plans, 237–238
  - investigating
    - about, 195–196
    - acquiring data, 198–200
    - containment, 202
    - cyber threat intelligence (CTI), 207–214
    - data processing and, 274–275
    - determining objectives, 197–198
    - eradicating, 202
    - evidence types, 223–228
    - GDPR and, 273–277
    - handling personal data during, 272
    - incidents, 196
    - malware analysis, 214–217
    - performing analysis, 200–202
    - policy for supporting, 272–273
    - preserving data, 198–200
    - reporting, 221–222
    - threat hunting, 218–221
  - investigation report, 221–222
  - ISACA, 40
  - ISO/IEC 27001 and 27002, 26–27, 37
  - issue-specific policies, 41–42
  - IT incident management, 156, 162
  - ITIL Strategy Management process, 27
- K**
- key performance indicators (KPIs), 188–189
  - key stakeholders
    - identifying, 42–43
    - introducing incident response teams to, 77–78
    - in Preparation phase of incident response lifecycle, 145
  - knowing your audience, 222
  - knowledge, 94, 186
- L**
- lateral movement, network artifacts in, 226–227
  - law enforcement, engaging, 251–252
  - lawful basis, 275
  - lawfulness, 274
  - legacy technology, 234

- legal and regulatory
  - considerations
    - about, 20, 243–244
    - admissibility of digital evidence, 258–265
    - breaches and, 244–252
    - collecting digital evidence, 252–258
    - compliance
      - considerations, 20–21
      - compliance requirements
        - for cyber breach response, 21–22
      - data privacy, 271–277
      - as a driver for cyber breach response, 20–22
      - establishing chain of custody, 265–271
      - forensic acquisition and legal requirement, 107
      - impact on cyber breach response of, 44
      - incident response teams and, 85–86
    - legal counsel, 85–86, 263–265
    - legal obligation, 275, 276
    - legitimate interest, 275, 276
    - lessons-learned
      - about, 180–181
      - meetings, 149–150, 183–184
      - process components, 181–183
    - lifecycles
      - cyber threat intelligence (CTI), 208–209
      - digital evidence, 253–258
      - incident response, 143–150
      - log management, 133–134
      - threat hunting, 219–221
      - vulnerability management, 178–179
    - litigation hold, 265
    - live acquisition, 106
    - live response, 106, 108–113, 268–269
    - “living off the land”
      - techniques, 121, 216
    - load balancing, 125
    - Lockheed Martin Cyber Kill Chain, 4
    - log management
      - about, 130, 132–133
      - in cloud computing environments, 117–118
      - collection and storage, 134–137
      - lifecycle of, 133–134
      - logging, 130–132
      - managing logs with a SIEM, 137–140
    - logged-on users artifacts, 225–226
    - logging, 130–132
    - logical acquisition, 104, 268–269
    - logistics, for remediation planning, 235
    - long-term containment, 148
    - low-fidelity indicators, 212
  - M**
  - Magnet ACQUIRE, 107
  - Maintain Persistence phase,
    - of cyberattack execution framework, 8
  - major incidents, 170–171
  - malware, 227, 250
  - malware analysis
    - about, 60–61, 214
    - classifying malware, 214–216
    - cyber threat intelligence and, 217
    - dynamic analysis, 217
    - static analysis, 216–217
  - Malware and Software Tools phase, of cyberattack preparation framework, 6
  - Managed level, in CMMI, 31
  - Management layer, of CSIRT coordinational model, 78–80
  - man-in-the-middle attack, 121
  - manual acquisition, 110
  - mapped drives and shares artifacts, 225
  - market conditions, impact on cyber breach response of, 44
  - materiality, in financial disclosure, 247–248
  - maturity assessment, 30–32
  - means, 248
  - media cloning, 267
  - meetings, conducting, 183–184
  - metrics, 153, 188
  - Microsoft Azure, 116, 117–118
  - Microsoft PowerShell, 110
  - mission statements, 32, 62
  - MITRE ATT&CK framework, 4
  - mobile device forensics, 204–205
  - monitoring, for attacker activity, 240–241
  - Morris, Robert Tappan (student), 52
  - “Morris Worm,” 52
  - motive, 248
  - Move Laterally phase, of cyberattack execution framework, 8
  - multifactor authentication (MFA), 57–58, 149, 238
  - multitenant architecture, 113
  - N**
  - National Health Service (NHS), xxv
  - National Institute of Standards and Technology (NIST), 13–14, 144
  - nation-state actors. *See* advanced persistent threats (APTs)
  - network activity artifacts, 225
  - network address translation (NAT), 204
  - network artifacts, 226–227
  - network connections artifacts, 225
  - network data, leveraging, 118–122
  - network flows, 118–119
  - network forensics, 204
  - Network Security Group (NSG) flow logs, 119
  - network worms, 215
  - NIST 800-53 Revision 4, 37
  - NIST Cyber Security Framework (CSF), 37
  - NIST SP 800-61 Revision 2, 163
  - no authority model, 76–77
  - non-forensic collection, 268
  - non-testifying expert privilege, 264–265
  - O**
  - objectives, 33, 197–198
  - observations, 10
  - open files artifacts, 226

open source tools, 98–99  
 Open state, for incidents, 168  
 Operation Tunisia, 3–4  
 operational functions, of  
 cybersecurity incident  
 response teams, 53  
 operational impact, 164, 165  
 operational intelligence, 19  
 Operational level, 46, 57  
 operational level  
 agreements (OLAs),  
 159–160  
 operational metrics, 27  
 operations, of cybersecurity  
 programs, 26–27  
 opportunity, 248  
 Optimizing level, in CMMI,  
 31  
 order of volatility, 103  
 Organization tier, for risk  
 management, 14  
 organized cybercrime, 3  
 osquery, 111  
 outsourcing, 89–94

## P

Payment Card Industry  
 Data Security Standard  
 (PCI DSS), 21–22, 37, 42,  
 122, 246–247  
 Payment Card Industry  
 (PCI) Security  
 Standards Council, 20  
 performance requirements,  
 for hardware, 101  
 periodic management  
 reports, 221  
 persistent artifacts, 223–225  
 personal data  
 defined, 273  
 handling during  
 investigations, 272  
 processing, 275–276  
 territorial transfer of,  
 276–277  
 personally identifiable  
 information (PII), 271  
 personnel, 69–75, 197  
 Plan, Do, Check, and Act  
 (PDCA), 184–185  
 Plan step, in Deming cycle,  
 184–185  
 planning  
 creating plans, 198  
 in Preparation phase of  
 incident response  
 lifecycle, 144–145  
 remediation, 233–238

platform-as-a-service (PaaS)  
 model, 114, 205  
 policies, 40–43, 162  
 Ponemon  
 Institute, xxv–xxvi  
 Post-Incident Activities  
 phase, of incident  
 response lifecycle,  
 149–150  
 post-incident evaluation  
 about, 177  
 lessons learned, 180–184  
 vulnerability  
 management,  
 177–180  
 postmortem. *See* post-  
 incident evaluation  
 Preparation phase, of  
 incident response  
 lifecycle, 144–145  
 Presentation phase, in  
 EDRM, 254, 258  
 preservation order, 265  
 Preservation phase, in  
 EDRM, 254, 255  
 preserving data, 198–200  
 proactive functions, 55–59  
 problem description, in  
 business case, 36  
 procedures  
 developing and  
 maintaining, 56  
 in execution plans, 237  
 process activities, 152–153  
 Process and Product  
 Quality Assurance  
 (PPQA), 30  
 process controls, 153–155  
 process custodian, 154–155  
 process data artifacts, 225  
 Process Data step, in  
 seven-step improvement  
 process, 187, 190–191  
 process documentation, 155  
 process enablers, 155  
 process feedback, 155  
 process improvements, 153  
 process integration, in  
 incident response  
 playbook workflow, 177  
 process interfaces, 155–158  
 process objective, 154  
 process owner, 154  
 process policy, 154  
 processing data, 100,  
 274–276  
 Processing phase  
 in CTI lifecycle, 208, 209  
 in EDRM, 254, 255–256

procuring hardware,  
 101–102  
 Production phase, in  
 EDRM, 254, 257  
 program execution  
 artifacts, 224  
 project steering committee,  
 as key stakeholders,  
 42–43  
 proxy servers, 120  
 public interest, 275  
 purple team exercises, 57  
 purpose limitation, 274

## Q

Quantitatively Managed  
 level, in CMMI, 31

## R

RACI chart, 159  
 Rackspace, 116  
 ransomware, 215  
 reactive functions, 59–61  
 readiness, assessing,  
 235–236  
 Recover Technology step, in  
 remediation workflow,  
 229–230  
 recovery, in incident  
 response playbook  
 workflow, 176  
 red team-blue team  
 exercises, 57  
 Reduce option, in risk  
 response, 180  
 relevance  
 of data, 190  
 Federal Rules of Evidence  
 (FRE) and, 259  
 reliability  
 of data, 190  
 Federal Rules of Evidence  
 (FRE) and, 259  
 Remediate stage, in  
 vulnerability  
 management lifecycle,  
 179  
 remediation  
 about, 147, 195–196, 228  
 containment and  
 eradication, 238–240  
 establishing a team,  
 230–232  
 monitoring for attacker  
 activity, 240–241  
 planning, 233–238  
 process of, 229–230  
 remediation lead, 231

- remediation owner, 232
  - Remote-Access Trojan (RAT), 215
  - Report stage
    - in threat hunting lifecycle, 220
    - in vulnerability management lifecycle, 179
  - report templates, 222
  - reporting, 133–134, 221–222
  - reproducibility, of data, 270
  - Request for Comments (RFC) 3227, “Guidelines for Evidence Collection and Archiving,” 103
  - requirements
    - establishing, 33–35
    - technology, 99
  - residual risk, managing, 17–18
  - Resolved state, for incidents, 168
  - resources, 155, 238
  - responsibilities, 82–90, 94
  - Responsible, in RACI chart, 159
  - retention, of incident response team personnel, 74–75
  - reverse proxy, 125
  - Reviewing phase, in EDRM, 254, 256
  - risk assessment, process of, 14–17
  - risk management
    - as a driver for cyber breach response, 13–18
    - impact on cyber breach response of, 44
    - integrating with vulnerability management, 180
  - risks, 2, 37
  - roadmaps, developing, 39
  - roles, 82–90, 94, 153, 158–159
  - runbooks. *See* incident response playbooks
- S**
- sandbox, 217
  - Sarbanes-Oxley Act (SOX), 21
  - scalability, log management and, 133
  - Scan for IOCs step, in analysis lifecycle, 201–202
  - Scope step, in threat hunting lifecycle, 220
  - scoping, 175, 226
  - script, 110
  - script kiddies, 4
  - security alerts, 227–228
  - security certifications, 72–73
  - security events, 131
  - security information and event management (SIEM), 134, 137–140, 161
  - Security Operations Center (SOC), 51, 54
  - Security Orchestration, Automation, and Response (SOAR) platforms, 139
  - security policy, 276
  - security requirements, for hardware, 101
  - security tools, 127–130
  - senior management, incident response teams and, 89–90
  - service desk, as a source of incident notifications, 161
  - service information artifacts, 226
  - service level agreements (SLAs), 159–160
  - service levels, in incident response plans, 159–160
  - seven-step improvement process, 187–192
  - severity, 163–167, 175
  - severity matrix, 166–167
  - shared authority model, 76
  - sharing knowledge, 94
  - short-term containment, 147
  - single-tier scheme, 163
  - situation room, 170
  - situational questions, 73
  - skills, as a prerequisite to threat hunting, 219
  - S.M.A.R.T. goals, 33
  - snapshot, 115
  - soft indicators, 212
  - soft skills, 71–72, 231
  - Software Engineering Institute (SEI), 30–31
  - software write blockers, 105
  - software-as-a-service (SaaS) model, 114
  - solution and benefits, in business case, 36
  - sources, 98–102, 160–162
  - spoliation, 265
  - standard operating procedures (SOPs). *See* incident response playbooks
  - standards, 246–247
  - static analysis, 216–217
  - storage limitation, 275
  - strategic assessment, as component in ITIL Strategy Management process, 28–32
  - strategic functions, of cybersecurity incident response teams, 53
  - strategic intelligence, 19
  - strategic level, of continual improvement, 45
  - strategic planning, 23–24
  - strategy, 1, 27–39
  - Strategy Definition step as component in ITIL Strategy Management process, 28, 32–37
    - in strategic planning, 23–24
  - strategy execution, as component in ITIL Strategy Management process, 28, 37–39
  - strengths, weaknesses, opportunities, and threats (SWOT), 29–30
  - Switch Port Analyzer (SPAN) port, 121–122
  - System and Organization Controls (SOC), 246–247
  - system artifacts, 223–226
  - system breach, 86
  - system events, 131
  - system memory acquisition, 105–106
- T**
- tabletop exercises, 57
  - tactical functions, of cybersecurity incident response teams, 53
  - tactical intelligence, 19
  - tactical level, of continual improvement, 45
  - target operating model (TOM), 25, 35
  - targeted acquisition, 104
  - targeted malware, 216
  - tasks, 169–170
  - technical analysis, 175

- technical groups, incident response teams and, 87–88
  - Technical level
    - of CSIRT coordinational model, 78–80
    - for incident response exercises, 57
  - technical reports, 221
  - technical skills, 69–71
  - technology
    - about, 97
    - commercial tools *vs.* open source tools, 98–99
    - forensic data, 102–113
    - identifying forensic evidence in enterprise technology services, 123–130
    - leveraging network data, 118–122
    - log management, 130–140
    - in Preparation phase of incident response lifecycle, 145
    - as a prerequisite to threat hunting, 218
    - for remediation planning, 234
    - skills and experience in, 231
    - sourcing, 98–102
    - virtualization, 113–118
  - technology group, 87
  - threat actors
    - about, 2–4
    - alerting, 236–237
    - eradicating, 148–149
    - monitoring for attacker activity, 240–241
    - network artifacts and visibility of, 227
    - as risk components, 16
  - threat hunting, 218–221
  - threats
    - continual improvement and, 45
    - cyberattack lifecycle, 4–8
    - as risk component, 16
    - threat actors, 2–4
  - Tier 1 support, 67
  - Tier 2 support, 67–68
  - Tier 3 support, 68
  - tiered model, 66–68
  - timelines, 175, 205–206
  - timeliness, of data, 190
  - timescale, in business case, 37
  - timestamping, 206
  - tools
    - for data, 191
    - for forensic imaging, 106–107
    - for live response, 109–112
    - security, 127–130
  - tools, tactics, and procedures (TTPs), 5, 70, 173, 200
  - total cost of ownership (TCO), 99
  - touchpoints, 93
  - tradecraft, 249
  - traditional forensic acquisition, 267–268
  - traditional virtualization, 113, 115
  - training personnel, 69–75, 145
  - transaction logs, 126
  - Transfer option, in risk response, 180
  - transparency, 274
  - triage, 173
  - tuning, tools for, 58–59
  - two-tier scheme, 163
- U**
- unauthorized access to resources, 228
  - unintentional insider threat, 3
  - United States, laws, regulations, and standards in, 245
  - urgency, 164, 166
  - U.S. Security and Exchange Commission (SEC), 247–248
  - use cases, 107–108, 112–113
- V**
- validating, 34, 190
  - vendors, establishing relationships with, 93–94
- Verify stage, in vulnerability management lifecycle, 179
- vertical communication, 63
  - Virtual Hard Disk (VHD) format, 116
  - virtual hosting, 125
  - virtual server
    - infrastructure (VSI) snapshots, 116
  - virtualization, 113–118
  - viruses, 215
  - VirusTotal, 214
  - vision statement, 32
  - vital interest, 275
  - volatile artifacts, 225–226
  - vulnerability, 16, 57–58, 228
  - vulnerability management, 157, 177–180
- W**
- WannaCry ransomware, xxv
  - war room, 170
  - warnings, 132
  - web application firewalls (WAFs), 127–128
  - web gateways, 120
  - web servers, 125–126
  - web shell, 128
  - web-based indicators, network artifacts and, 227
  - Windows Event Collector, 135
  - Windows Event Forwarder, 135
  - Wisdom, in DIKW hierarchy, 186
  - work instructions, 153
  - workflow, 160–171, 173–177
  - World Economic Forum, xxvi
  - write blockers, 105
  - writing, in formal language/active voice, 222
- X**
- X-Ways Forensics, 107
- Y**
- Yahoo!, 248