INDEX

A

- ABAC (Attribute-Based Access Control), 396
- ABSN (autonomous body sensor network), 143
- acceptable use policy (AUP), 441–442
- acceptance, 461
- access control
  - concepts, 391–392
  - poor, 391–397
  - roles and terminology, 393
  - schemes, 392–396
    - Attribute-Based Access Control (ABAC), 396
    - Discretionary Access Control (DAC), 394, 418–419
    - Mandatory Access Control (MAC), 394–395
    - Role-Based Access Control (RBAC), 395–396
    - Rule-Based Access Control, 396
  - steps in, 392
- access control list (ACL), 266, 396–397
- access point (AP), 325
  - captive portal, 327
  - configuration, 338–339
  - evil twin, 328–329
  - fat *vs.* thin, 325–326
  - probe, 339
  - rogue, 328
  - standalone *vs.* controller, 326
  - wireless LAN controller (WLC), 326–327
- access policy, 437
- access technologies, 266–269
  - access control list (ACL), 266
  - data loss prevention (DLP), 268–269
  - network access control (NAC), 267–268
  - virtual private network (VPN), 266–267
- account audits, 438
- accounting, 392
- account management policies, 437–439
- account permissions, 437
- ACL (access control list), 266, 396–397
- active-active configuration, 276
- Active Directory, 437–438
- active-passive configuration, 275
- active reconnaissance, 40
- actor, threat, 7–8, 10
- address resolution protocol (ARP), 230, 307
  - poisoning, 229–230
- ad fraud attack, 73
- ad hoc mode, 325
- admissibility, 407
- advanced encryption standard (AES), 167
- advanced persistent threat (APT), 10
- adversarial artificial intelligence, 85
- adversarial artificial intelligence attacks, 83
  - artificial intelligence (AI), 84
  - machine learning (ML), 84
  - risks in using AI and ML in cybersecurity, 85
  - uses in cybersecurity, 84–85
- adversary tactics, techniques, and procedures (TTP), 54
- AES (advanced encryption standard), 167
- AES-CCMP encryption, 334
- affinity scheduling, 275
- agentless NAC, 267
- agents, 267
- aggregators, 272
- agile model, 114
- AH protocol (Authentication Header) protocol, 210
- AI (artificial intelligence), 83
  - in cybersecurity, 84–85
  - defining, 84
- AICPA (American Institute of Certified Public Accountants), 51
- air gap, 244
- AIS (Automated Indicator Sharing), 97
- alarm, 242
- ALE (Annualized Loss Expectancy), 459
- algorithm, 159
- algorithm attacks, 173
- always-on VPNs, 267
- Amazon Web Services (AWS), 289, 293
- American Institute of Certified Public Accountants (AICPA), 51
- analog meters *vs.* smart meters, 142
- android smart lock configuration options, 138
- annual credit report, 474–475
- Annualized Loss Expectancy (ALE), 459
- Annualized Rate of Occurrence (ARO), 459
- anomaly-based monitoring, 264
- anomaly monitoring, 263
- antennas, 40, 348
- anticlimb collar, 240
- anticlimb paint, 240
- antimalware, 104
- antispyware, 104
- antivirus (AT), 103–104
- anything as a service (XaaS), 291–292
- AP (access point), 325
  - captive portal, 327
  - configuration, 338–339
  - evil twin, 328–329
  - fat *vs.* thin, 325–326
  - probe, 339
  - rogue, 328
  - standalone *vs.* controller, 326
  - wireless LAN controller (WLC), 326–327
- API (application program/protocol interface), 98, 234
- API attack (application program interface attack), 83
- app data, 412
- appender infection, 70
- Apple touch gestures, 130
- appliance firewall, 259, 260
- appliance OS, 109
- application attacks, 77–78
  - attacks on software, 81–83
  - injection, 78–79
  - replay, 80
  - request forgery, 80
  - scripting, 78
- application development concepts, 114
  - general concepts, 114
  - SecDevOps, 114–115
- application development lifecycle model, 114
- application management, 139
- application program/protocol interface (API), 98, 234
  - attack, 83
  - defining, 84
- application security, 295
- application whitelisting/blacklisting, 110
- APT (advanced persistent threat), 10
- archive bit, data backup, 434, 448
- Arduino, 140
- armored file-based virus, 71
- ARO (Annualized Rate of Occurrence), 459
- ARP (address resolution protocol), 229–230, 307
- ARP poisoning, 271
  - attack, 230
- artifacts, 407
- artificial intelligence (AI), 83
  - cybersecurity, 84–85
  - defining, 84
- assessment and defense, tools for, 236–237
  - Linux file manipulation tools, 238
  - network reconnaissance and discovery tools, 237–238
  - packet capture and replay tools, 238–239
  - scripting tools, 238
- asset inventory, 44
- asset management
  - Nessus hardware, 44
  - Nessus software, 44
  - policy, 442
- asset value, 455
- asymmetric cryptographic algorithms, 168–169
- asymmetric cryptography, 192
- asymmetric server cluster, 428
- AT (antivirus), 103–104
- ATM (automated teller machine), 274
- attacker, 7
- attacks. *See also specific types of attack*
  - based on application vulnerabilities, 113
  - impacts of, 21
    - data impacts, 21
    - effects on the enterprise, 21–22
  - using malware, 66–69
- attacks on networks, 226–227
  - distributed denial of service attack, 233–234
  - DNS attacks, 231–233
    - DNS hijacking, 232–233
    - DNS poisoning, 232

Copyright 2022 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

- attacks on networks (*Continued*)
  - interception attacks, 227
    - man-in-the-browser (MITB), 228
    - man-in-the-middle (MITM), 227
    - session replay, 227–228
  - layer 2 attacks, 228–230
    - address resolution protocol poisoning, 229–230
    - media access control attacks, 230–231
  - malicious coding and scripting attacks, 234
    - Bash, 236
    - PowerShell, 234
    - Python, 236
    - visual basic for applications (VBA), 234–236
- attacks on software, 81–83
  - external software components, 83
  - improper exception handling, 82
  - memory vulnerabilities, 81–82
- attack vectors, 14–15
- attestation, 364
- attestation mechanism, 114
- Attribute-Based Access Control (ABAC), 396
- attributes, 8, 355
- AUP (acceptable use policy), 441–442
- authentication, 136, 354–355
  - biometrics, 364
    - analysis, 386
    - behavioral, 368–369
    - cognitive, 367–368, 384–385
    - disadvantages, 367
    - laws, 387
    - physiological, 365–367
    - specialized scanners, 365–366
  - constraint, 144
  - context-aware, 137
  - framework protocols, 377
  - by keystroke dynamics, 368, 369, 383
  - log in with other sites, 387
  - passcode, 136–137
  - password, 355
    - attacks on, 357–361
    - generators, 371
    - management applications, 371–372, 386
    - online password cracker, 382
    - protecting digests, 370–371
    - requirements, 386
    - security, 370–372
    - vault, 371–372, 384
    - weaknesses, 356–357
  - screen lock, 137
  - secure technology, 373–377
  - services, 373–377
  - single-factor, 361
  - smartphones, 363–364
  - specialized devices, 361
    - security keys, 364
    - smart card, 361–362
    - windowed tokens, 362–363
  - Windows Picture Password, 367, 385
- authentication app, 363
- authentication constraint, 144
- Authentication Header (AH) protocol, 210
- authentication mode of operation, 213
- authentication request, 374
- authentication servers, 403
- authority, 15
  - certificate, 194
  - registration, 194
- authorization, 38, 392
- automated courses of action, 115
- Automated Indicator Sharing (AIS), 97
- automated patch update service, 107–108
- automated teller machine (ATM), 274
- automatic continuous backup, 435
- automatic download software, 73
- autonomous body sensor network (ABSN), 143
- Autopsy, 411
- auto-update, 107
- availability, information security, 6
- availability loss, 21
- avoidance, risk, 461
- AWS (Amazon Web Services), 289, 293

B

- backdoor, 76
- background checks, 441
- backup copy, 435
- backups, 433, 447–448
  - archive bit, 434, 448
  - calculations, 433
  - online backup services, 451
  - personal backup procedures, 451
  - storing, 435–436
  - types of, 433, 434
- badge, 244
- BAN (body area networks), 143
- barricade, 240
- baseband, 339
- baseline configuration, 265
- Bash, 236
- Basic Input/Output System (BIOS), 101
- Bayesian filtering, 104
- BBC (British Broadcasting Corporation), 294
- BCP (business continuity plan), 425–426
  - elements, 425–426
  - goals, 425
  - terminology, 425
- behavioral monitoring, 264
- behavior-based monitoring, 264
- benchmark/secure configuration guides, 54
- BIA (business impact analysis), 426–427, 451
- binary, 114
- biometrics, 137, 364
  - analysis, 386
  - behavioral, 368–369
  - cognitive, 367–368, 384–385
  - disadvantages, 367
  - laws, 387
  - physiological, 365–367
  - specialized scanners, 365–366
- BIOS (Basic Input/Output System), 101
  - attack, 102
  - firmware, 101
- BioStar 2, 353–354
- birthday attack, 174, 360
- bits per second (bps), 320
- bit-stream backup, 408
- black box, penetration testing levels, 37
- black hat hackers, 8
- blacklisting, 110
- blockchain, cryptography, 178–179
- block cipher, 164
- block cipher mode of operation, 213–214
- blocker ransomware, 67
- Blowfish, 167
- bluejacking attacks, 320
- bluesnarfing attacks, 321
- blue team, penetration testing war game, 36
- Bluetooth, 319–321
  - products, 319
  - range estimator, 347–348
- Bluetooth Basic Rate/Enhanced Data Rate (BR/EDR), 320
- body area networks (BAN), 143
- bollard, 240–241
- Boomer Barons, 467
- boot attestation, 103
- boot integrity, 101–103
- boot security, 102–103
- bot, 72–73
- BPA (business partnership agreement), 463
- BPDU (bridge protocol data units), 270
- bps (bits per second), 320
- BR/EDR (Bluetooth Basic Rate/Enhanced Data Rate), 320
- bridge protocol data units (BPDU), 270
- bridge trust model, 203–204
- bring your own device (BYOD), 133
- British Broadcasting Corporation (BBC), 294
- broadcast storm prevention, 270
- brokers, 10
- browsers, web, 104–105
- brute force attack, 358
- buffer overflow attack, 81–82
- bug bounty, 37
- burning, 470
- business continuity, 424, 425
  - business continuity plan (BCP), 425–426
  - business impact analysis (BIA), 426–427, 451
  - disaster recovery plan (DRP), 427
  - percentage availability and downtimes, 426
  - resilience through redundancy
    - data, 433–436
    - disks, 428–431
    - endpoints, 427–428
    - networks, 431
    - power, 431–432
    - servers, 428
    - sites, 433
- business continuity plan (BCP), 425–426
  - elements, 425–426
  - goals, 425
  - terminology, 425
- business impact analysis (BIA), 426–427, 451
- business partners, 462
- business partnership agreement (BPA), 463
- business recovery planning, 425
- BYOD (bring your own device), 133

C

- CA (certificate authority), 194
- cable lock, 245

Copyright 2022 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

CAC (common access card), 361
cache, 408
CALEA (Communications Assistance for Law Enforcement Act of 1994), 52
California's Database Security Breach Notification Act, 53
call detail records, 412
call manager, 403
CAM (content addressable memory), 231
candidates, 358
Canonical Encoding Rules (CER), 200
capacitive technology, 365
capture the flag (CTF), 465
card cloning, 362
carrier unlocking, 136
CASB (cloud access security broker), 295
CBC (Cipher Block Chaining), 213
CBT (computer-based training), 465
C&C (command and control), 73
CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), 334
CCTV (closed circuit television), 241
CDP (continuous data protection), 434, 451
cellular telephony, 132
Center for Internet Security (CIS), 51, 115
CER (Canonical Encoding Rules), 200
CER (crossover error rate), 367
.cer extension, 200
certificate
  authorities, 194
  management, 195–196
certificate attributes, 200
certificate authority (CA), 194
  intermediate, 194
  offline CA, 194
  online CA, 194
certificate chaining, 197
certificate life cycle, 205
certificate policy (CP), 204
certificate practice statement (CPS), 204–205
certificate repository (CR), 195
certificate revocation, 195
  web browser, 196
Certificate Revocation List (CRL), 195
certificates, digital
  attributes and formats, 200–201
  certificate management, 195–196
  code signing digital certificate, 200
  defining, 192–193
  domain digital certificates, 198–199
  domain validation, 199
  elements, 194
  email, 200
  extended validation (EV) certificate, 199
  hardware digital certificates, 199–200
  machine/computer digital certificate, 199
  management, 194–196
    certificate authorities, 194
    certificate management, 195–196
  root digital certificates, 197–198
  software digital certificates, 199–200
  types, 197–201
  wildcard, 199
certificate signing request (CSR), 194
Certified Public Accountants (CPAs), 51
CFAA (Computer Fraud and Abuse Act), 52
chain, 360
chain of custody, 407, 408
Challenge-Handshake Authentication Protocol (CHAP), 377
change control policy, 442
change management policy, 442
channel overlays, 338
CHAP (Challenge-Handshake Authentication Protocol), 377
Chemical Facility Anti-Terrorism Standards Regulation, 52
chief information officer (CIO), 4
chief information security officer (CISO), 4
Children's Online Privacy Protection Act (COPPA), 52
choose your own device (CYOD), 133
CIA (confidentiality, integrity, and availability), 6
CIO (chief information officer), 4
cipher, 159, 160
  block, 164
  stream, 164
Cipher Block Chaining (CBC), 213
Cipher Block Chaining Message Authentication Code (CBC-MAC), 334
cipher suite, 208
ciphertext-only attack, 173
CIS (Center for Internet Security), 51, 115
CISA (Cybersecurity and Infrastructure Security Agency), 99
CISA (Cybersecurity Information Sharing Act), 98
CISCA (Cyber Information Sharing and Collaboration Agreement), 97, 98
CISCP (Cyber Information Sharing and Collaboration Program), 97
CISO (chief information security officer), 4
clean desk space, 440
cleanup, rules of engagement, 39
client-side execution and validation, 116
client-side request forgery, 80
cloning attack, MAC, 231
closed circuit television (CCTV), 241
cloud access security broker (CASB), 295
Cloud App Security, 438–439
cloud architecture, 289
cloud backup, 435
cloud computing, 286
  advantages, 287
  characteristics, 287
  cloud architecture, 289
  cloud types, 288
  defining, 286–287
  features, 288
  locations, 288–289
  management, 291–292
    local management, 292
    service providers, 292
  models, 289–292
    anything as a service (XaaS), 291–292
    infrastructure as a service (IaaS), 290–291
    platform as a service (PaaS), 290
    software as a service (SaaS), 289–290
  security, 292–298
    application security, 295
    issues, 292–298
    security controls, 293–295
    security virtual device solutions, 296–298
cloud conceptual model, 298, 315
Cloud Controls Matrix, 52
cloud firewall, 296
cloud forensics, 420
cloud native controls, 293
cloud platforms, 12
cloud security
  application security, 295
  issues, 292–298
  security controls, 293–295
  security virtual device solutions, 296–298
Cloud Security Alliance (CSA), 52
cloud security audit, 293
cloud service providers, 287
cloud storage, 424
cloud types, 288
clustering, 428
CMOS (complementary metal-oxide-semiconductor), 101
CN (common name), 200
code reuse of third-party libraries and SDKs, 116
code signing, 116
code signing digital certificate, 200
code testing, 115
  dynamic code analysis, 116, 118
  static code analysis, 116, 117
cognitive biometrics, 367–368, 384–385
  memorable event, 386
cold site, 433
collectors, 272
collision attacks, 173–174
command and control (C&C), 73
common access card (CAC), 361
common name (CN), 200
Common Vulnerabilities and Exposures (CVE), 46, 67
Common Vulnerability Scoring System (CVSS), 47
communication plan, 398
communication, rules of engagement, 39
Communications Assistance for Law Enforcement Act (CALEA) of 1994, 52
community cloud, 288
compensating control, 462
competitors, 10
compilers, 114
complementary metal-oxide-semiconductor (CMOS), 101
CompTIA Security + SY0-601 Certification Exam Objectives, 479–503
compute constraint, 144
computer-based training (CBT), 465
computer contaminant, 66
Computer Fraud and Abuse Act (CFAA), 52
computer hardware security, 245–246
computer incident monitoring organizations, 459
Computing Technology Industry Association (CompTIA) Security+ certification, 4–5

Copyright 2022 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

conditional access, 396
confidential data, 469
confidentiality, information security, 6
confidentiality, integrity, and availability (CIA), 6
configuration management, security appliances, 265
configuration review, 45
confinement tools, 110–111
consensus, 15
constraints, 144
  cryptographic, 163
consumer attacks, wireless local area network (WLAN), 330–331
contactless payment systems, 321, 322, 347
container, 299
containerization, 138
container security, 303
containment, incident response process, 397
content addressable memory (CAM), 231
content inspection, 268
content management, 139
content/URL filtering, 258
context-aware authentication, 137
continual vulnerability scans, 43
continuity of operation planning (COOP), 426
continuous data protection (CDP), 434, 451
continuous delivery, 115
continuous deployment, 115
continuous integration, 115
continuous monitoring, 115
continuous validation, 115
control attacks, media access, 230–231
control risk, 462
convenience, security and, 5
COOP (continuity of operation planning), 426
COPE (corporate owned, personally enabled), 133
COPPA (Children's Online Privacy Protection Act), 52
corporate owned, personally enabled (COPE), 133
corrective control, 462
cost constraint, 144
counter (CTR) mode, 213
Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), 334
covered writing, 159
COVID-19 pandemic, 453–454
CP (certificate policy), 204
CPAs (Certified Public Accountants), 51
CPS (certificate practice statement), 204–205
CR (certificate repository), 195
credentialed scan *vs.* non-credentialed scans, 45
credential harvesting, 16
credential policies, 437
credentials. *See* authentication
criminal syndicates, 10
crisis management and communications, 425
critical data, 469
CRL (Certificate Revocation List), 195
crossover error rate (CER), 367
cross-site request forgery (CSRF), 80
cross-site scripting (XSS) attack, 78
crowdsourced pen testers, 37
cryptographic protocols, 207–208
  Hypertext Transport Protocol Secure (HTTPS), 209
  Internet Protocol Security (IPsec), 210
  Secure/Multipurpose Internet Mail Extensions (S/MIME), 209
  Secure Real-Time Transport Protocol (SRTP), 209
  Secure Shell (SSH), 208
  Secure Sockets Layer (SSL), 208
  Transport Layer Security (TLS), 208
  weaknesses of, 210
cryptography, 158–160
  algorithms, 164–165
    asymmetric cryptographic algorithms, 168–169
    hash algorithms, 165–166
    symmetric cryptographic algorithms, 166–167
  asymmetric, 192
  attacks on, 173
    algorithm attacks, 173
    collision attacks, 173–174
  authentication, 161
  blockchain, 178–179
  confidentiality, 160–161
  constraints, 144, 163
  encryption through software, 175–177
    file and file system cryptography, 176
    full disk encryption (FDE), 176
  hardware encryption, 177
    hardware security module (HSM), 177, 178
    self-encrypting drives (SEDs), 177
    trusted platform module (TPM), 177–178
    USB device encryption, 177
  implementing, 211
    block cipher modes of operation, 212–213
    crypto service providers, 213
    key strength, 211–212
    secret algorithms, 212
  information protections by, 161
  integrity, 161
  lightweight, 163
  limitations of, 162–163
  nonrepudiation, 161
  obfuscation, 161
  post-quantum, 175
  quantum cryptographic defenses, 174–175
  using, 175–179
cryptomalware, 68–69
crypto service providers, 213
CSA (Cloud Security Alliance), 52
CSF (Cybersecurity Framework), 51
CSR (certificate signing request), 194
CSRF (cross-site request forgery), 80
CTF (capture the flag), 465
C-TPAT (Customs-Trade Partnership Against Terrorism), 52
CTR (counter mode), 213
Cuckoo, 238
curl (Linux), 237
custom firmware, 136
Customs-Trade Partnership Against Terrorism (C-TPAT), 52
CVE (Common Vulnerabilities and Exposures), 46, 67
CVSS (Common Vulnerability Scoring System), 47
cyberattacks, 4, 8
cybercrime, 4
  financial, 8
Cyber Information Sharing and Collaboration Agreement (CISCA), 97
Cyber Information Sharing and Collaboration Program (CISCP), 97
  privacy protections, 97, 98
Cyber kill Chain, 400
cybersecurity, 4
  artificial intelligence (AI), 84–85
  framework core elements, 50
  machine learning (ML) in, 85
  resource, 52
  vulnerabilities, 11
Cybersecurity and Infrastructure Security Agency (CISA), 99
Cybersecurity Framework (CSF), 51
Cybersecurity Information Sharing Act (CISA), 98
cybersecurity insurance, 461
cyberterrorists, 10
CYOD (choose your own device), 133

D

DAC (Discretionary Access Control), 394, 418–419
DAP (Directory Access Protocol), 306
dark web, 100
dashboard, HIDS, 105–106
data, 433–436
data anonymization, 469
data at rest, 162
data attack, consequences of, 22
data backup, 433, 447–448
  archive bit, 434, 448
  calculations, 433
  online backup services, 451
  personal backup procedures, 451
  storing, 435–436
  types of, 433, 434
data breach, 22
data breach consequences, 468
data breach notification law, 413
data classification policy, 442–443
data controller, 393
data custodian/steward, 393
data destruction, 470
data encryption standard (DES), 166
data exfiltration, 22
data exposure, 115
data feeds, 54
data governance policy, 443
data hidden by steganography, 159
data in processing, 162
data in transit, 162
data loss, 22
data loss prevention (DLP), 268–269

Copyright 2022 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

data management tools, 47
  Security Information and Event Management (SIEM), 48–49
  Security Orchestration, Automation, and Response (SOAR), 49
data masking, 469
data minimization, 468
data owner, 393
data policies, 442–443
data privacy, 466–470
  data breach consequences, 468
  data destruction, 470
  data types, 468, 469
  protecting data, 468–470
  user concerns, 467
data privacy officer (DPO), 393
data processor, 393
data protection, 468–470
data retention policy, 443
data sovereignty, 469
data storage, 13
dd (GNU dd), 411
DDoS attack (distributed denial of service attack), 233–234
dead code, 116
deceive, 75–76
  potentially unwanted program (PUP), 75–76
  remote access Trojan (RAT), 76
  Trojan, 76
decision-making, biases and effects, 457–460
decryption, 159
dedicated probe, 339
default settings, configurations, 12
defenses, quantum cryptographic, 174–175
degaussing, 470
delayed deletion, 435
demilitarized zone (DMZ), 244, 274
denial of service (DoS) attack, 330
deprovisioning, 114
DER (Distinguished Encoding Rules), 200
DES (data encryption standard), 166
design technologies, 272
  load balancing, 275–276
  network segmentation, 272–275
desktop probe, 339
detective control, 462
deterrent control, 462
development stage, 114
device driver manipulation, 83
DevOpsSec. *See* SecDevOps
DevSecOps. *See* SecDevOps
DHCP (Dynamic Host Configuration Protocol), 270
  servers, 403
  snooping, 270
DHE (Diffie-Hellman Ephemeral key exchange), 172
diagram, 265
Diamond Model of Intrusion Analysis, 399, 420
dictionary attack, 359–360
differential backup, 434
Diffie-Hellman Ephemeral (DHE) key exchange, 172
Diffie-Hellman (DH) key exchange, 172
dig (Linux), 237
digital certificates
  attributes and formats, 200–201
  certificate management, 195–196
  code signing digital certificate, 200
  defining, 192–193
  domain digital certificates, 198–199
  domain validation, 199
  elements, 194
  email, 200
  Extended Validation (EV) certificate, 199
  hardware digital certificates, 199–200
  machine/computer digital certificate, 199
  management, 194–196
    certificate authorities, 194
    certificate management, 195–196
  root digital certificates, 197–198
  software digital certificates, 199–200
  types, 197–201
  wildcard, 199
digital forensics, 405
  cloud forensics, 412–413
  procedures, 405–412
    document chain of custody, 407
    enable recovery, 410
    examine for evidence, 407–410
    preservation of the evidence, 406–407
    secure the scene, 405–406
    tools, 410–412
  workstation, 411, 412
digital malware analysis, 97
digital signature, 192, 193
digital signature algorithm (DSA), 170–171
direct access vector, 14
Directory Access Protocol (DAP), 306
directory service, 306, 376
directory traversal attack, 113
disablement, 439
disabling unnecessary open ports and services, 108
disassociation attack, 330
disaster recovery, 425
disaster recovery plan (DRP), 427
disasters, 424
Discretionary Access Control (DAC), 394, 418–419
disk duplexing, 430
disk mirroring, 430
disks, 428–431
dissolvable NAC agent, 267
distance considerations, 435
Distinguished Encoding Rules (DER), 200
distributed denial of service (DDoS) attack, 233–234
distributed trust model, 203
diversity, business continuity plan, 426
DLL (dynamic-link library), 83
DLL injection, 83
DLP (data loss prevention), 268–269
DMZ (demilitarized zone), 244, 274
DNS (Domain Name System), 403
DNS attacks, 231–233
dnsenum, 238
DNS hijacking, 232–233
DNS poisoning, 232
DNSSEC (Domain Name System Security Extensions), 304–305
DNS sinkhole, 263
documented incident, 397
domain name resolution, 231
domain name server (DNS) caches, 49
domain name server (DNS) memory, 18
domain name system (DNS), 231, 403
Domain Name System Security Extensions (DNSSEC), 304–305
domain reputation, 231
domain validation digital certificate, 199
DoS (denial of service) attack, 330
downgrade attack, 173
download harmful content, 331
downtimes, percentage availability and, 426
DPO (data privacy officer), 393
drive file slack, 410
drones, 40, 41, 143
DRP (disaster recovery plan), 427
DSA (digital signature algorithm), 170–171
dual power supply, 431, 432
dump file, 403, 404
dumpster diving, 20–21
dwell time, 368
dynamic analysis, 104
dynamic code analysis, 116
dynamic fingerprint scanner, 365, 366
Dynamic Host Configuration Protocol (DHCP), 270
dynamic-link library (DLL), 83

E

EAP (Extensible Authentication Protocol), 335, 348, 377
EAP-FAST, 335
EAP-TLS, 335
EAP-TTLS, 335
east-west traffic, 273
ECB mode (Electronic Code Book mode), 213
ECC (elliptic curve cryptography), 169–170
Echo request packets, 405
ECPA (Electronic Communications Privacy Act of 1986), 52
edge, 288
e-discovery, 407
EDR (endpoint detection and response), 106–107
EEA (European Economic Area), 52
EF (Exposure Factor), 459
efficacy rate, 367
elasticity, 115
  cloud computing, 288
electromagnetic interference (EMI), 245
Electronic Code Book (ECB) mode, 213
Electronic Communications Privacy Act (ECPA) of 1986, 52
Electronic Fund Transfer Act, 52
electronic lock, 243
eliciting information, 15
elliptic curve cryptography (ECC), 169–170
email client, 306
email digital certificate, 200
email servers, 403

Copyright 2022 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

- embedded system, 140
  - device types, 140–144
    - hardware and software, 140–141
    - industrial systems, 142
    - Internet of Things (IoT), 143–144
    - specialized systems, 141–143
  - security constraints for, 144
  - security issues, 144–145
- EMEC (European Marine Energy Center), 285
- EMI (electromagnetic interference), 245
- Encapsulating Security Payload (ESP) protocol, 210
- EnCase software, 411
- encryption, 159
- end of life (EOL), 463
- end of service (EOS), 463
- endpoint detection and response (EDR), 106–107
- endpoints, 66, 427–428
- enterprise attacks, wireless local area network (WLAN), 327–330
- enterprise method, 334
- entropy, 163
- environmental disasters, 425
- EOL (end of life), 463
- EOS (end of service), 463
- ephemeral keys, 172
- eradication, incident response process, 397
- error handling, 82
- errors, configurations, 13
- escalation, 468
- ESP protocol (Encapsulating Security Payload protocol), 210
- European Economic Area (EEA), 52
- European Marine Energy Center (EMEC), 285
- European Union General Data Protection Directive (GDPR), 52
- evade, 76–77
  - backdoor, 76
  - logic bomb, 76
  - rootkit, 76
- EV certificate (Extended Validation certificate), 199
- evil twin, 328
- executable files attack, 113
- exercises, 398
- expiration, 206
- exploitation
  - frameworks, 399
  - rules of engagement, 39
- Exposure Factor (EF), 459
- Extended TACACS (XTACACS), 375
- extended validation (EV) certificate, 199
- Extensible Authentication Protocol (EAP), 335, 348, 377
- eXtensible Markup Language (XML), 79
- external disasters, 425
- external media access, 135
- external perimeter defenses
  - barriers, 240–241
  - personnel, 241–242
  - sensors, 242–243
- external risk, 456
- external threat actor, 8
- extranet, 275

F

- facial recognition, 367
  - software with federation technology, 382–383
- FACTA (Fair and Accurate Credit Transaction Act), 52
- factors, 355
- FAF (Firm and Fit), 476–477
- failure in time (FIT), 458
- Fair and Accurate Credit Transaction Act (FACTA), 52
- Fake RAID, 429
- fake telemetry, 262
- false acceptance rate (FAR), 367
- false negative, 47
- false positive, 47
- false rejection rate (FRR), 367
- familiarity, 16
- Family Educational Rights and Privacy Act (FERPA), 468
- FAR (false acceptance rate), 367
- Faraday cage, 246
- FAST (Free and Secure Trade Program), 52
- fat APs, 326
- fault tolerance, 427
- FBI (Federal Bureau of Investigation), 99
- FDE (full disk encryption), 137, 176
- Federal Bureau of Investigation (FBI), 99
- Federal Information Security Management Act (FISMA), 52
- Federal Intelligence Surveillance Act (FISA) of 1978, 52
- Federal Privacy Act of 1974, 52
- Federal Rules of Civil Procedure (FRCP), 52
- federated identity management (FIM), 373
- federation, 373, 382–383
- fencing, 240
- FERPA (Family Educational Rights and Privacy Act), 468
- field-programmable gate array (FPGA), 141
- file and code repositories, 99
- file backup, 434
- file-based encryption, 137
- file-based virus, 69–71
  - advantages of, 71–72
  - armored, 71
- file integrity monitors, 272
- fileless virus, 71–72
- filesystem ACLs, 266
- filesystem permissions, 396
- File Transfer Protocol (FTP), 305–306
- FIM (federated identity management), 373
- financial cybercrime, 8
- financial loss, 21
- fines, 468
- fingerprint, 365
- fire suppression, 245
- firewalls, 257, 403
  - categories, 258–260
  - functions, 257–258
  - open source *vs.* proprietary, 259
  - rule actions, 257
  - specialized firewall appliances, 260–261
  - stateful *vs.* stateless, 258–259
- Firm and Fit (FAF), 476–477
- firmware, 14, 409
  - BIOS, 101
  - custom, 136
- firmware over-the-air (OTA) updates, 134
- first-party cookie, 105
- FISA (Federal Intelligence Surveillance Act of 1978), 52
- FISMA (Federal Information Security Management Act), 52
- FIT (failure in time), 458
- fitness tracker, 131
- 5G, 339
- flight time, 368
- flooding attack, MAC, 231
- fog, 288
- FOIA (Freedom of Information Act), 98
- footprinting, 40
- forensics, 405
  - cloud, 412–413, 420
  - data sources, 420
  - hardware tools, 411–412
  - procedures, 405–412
    - document chain of custody, 407
    - enable recovery, 410
    - examine for evidence, 407–410
    - preservation of the evidence, 406–407
    - secure the scene, 405–406
    - tools, 410–412
  - software tools, 411
- forward proxy, 261
- FPGA (field-programmable gate array), 141
- frameworks, 50
  - American Institute of Certified Public Accountants (AICPA), 51
  - Center for Internet Security (CIS), 51
  - cybersecurity framework core elements, 50
  - International Organization for Standardization (ISO), 51
  - National Institute of Standards and Technology (NIST), 50–51
- FRCP (Federal Rules of Civil Procedure), 52
- Free and Secure Trade Program (FAST), 52
- Freedom of Information Act (FOIA), 98
- frequency band, 338
- FRR (false rejection rate), 367
- FTK Imager, 411
- FTP (File Transfer Protocol), 305–306
- FTPS (FTP Secure), 305
- full backup, 434
- full disk encryption (FDE), 137, 176
- full tunnel, 267
- functional recovery plan, 426
- fusion center, 49
- fuzzer input generator, 118
- fuzzing, 116

G

- gait, 366
- Galois/Counter (GCM) mode, 213
- gamification, 465
- GCM mode (Galois/Counter mode), 213
- General Data Protection Directive (GDPR), 52
- General Data Protection Regulation, 468
- generator, 432

Copyright 2022 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

generic account, 391
geofencing, 139, 439
geographic dispersal, 433
geolocation, 135, 439
geo-tagging, 135, 439
GLBA (Gramm-Leach-Bliley Act), 52, 468
global positioning system (GPS), 135
  data, 412
  receiver, 40
  tagging, 135
GNU dd (dd), 411
Gramm-Leach-Bliley Act (GLBA), 52, 468
gray box, penetration testing levels, 37
gray hat hackers, 8
Group Policy, 437, 438
guest account, 391
guest network, 275
guest systems, 297

H

hackers, 8
  black hat, 8
  gray hat, 8
  types, 8
  white hat, 8
hacktivists, 9
Hard Chargers, 467
hard disk drives (HDDs), 429
harden endpoints, 107
  operating systems, 108–112
  patch management, 107–108
hardware digital certificates, 199–200
hardware firewalls, 259
hardware modules, 372
hardware root of trust, 103
hardware security module (HSM), 177, 265
hash algorithms, 165–166
hashing, 165
HDDs (hard disk drives), 429
Health Information Technology for Economic and Clinical Health Act (HITECH), 52
Health Insurance Portability and Accountability Act of 1996 (HIPAA), 52, 288, 468
heating, ventilation, and air conditioning (HVAC) environmental systems, 142
heat map, 337
heuristic monitoring, 264
hidden data, windows slack and, 418
hidden writing, 159
HIDS (host intrusion detection system), 105–106, 264
hierarchical trust model, 202–203
high availability across zones, 293
high availability, business continuity plan, 425
high resiliency, 163
HIPAA (Health Insurance Portability and Accountability Act), 52, 288, 468
HIPS (host intrusion prevention system), 106
HITECH (Health Information Technology for Economic and Clinical Health Act), 52
HMAC-based one-time password (HOTP), 363
hoaxes, 20
honeyfiles, 262
honeynet, 262
honeypot, 262
host-based firewall, 259
hosted services, 286
hosted services environment, 12
host intrusion detection system (HIDS), 105–106, 264
host intrusion prevention system (HIPS), 106
host system, 297
host virtualization, 297
hot aisle/cold aisle, 244
HOTP (HMAC-based one-time password), 363
hot site, 433
hotspots, 135
hping (Linux), 237
HTML 5, 267
HTTP (Hypertext Transfer/Transport Protocol), 77, 104, 105
HTTP response headers, 105
HTTPS (Hypertext Transfer Protocol Secure), 98, 209
HVAC environmental systems (heating, ventilation, and air conditioning environmental systems), 142
hybrid attack, 360
hybrid cloud, 288
hybrid warfare influence campaign, 15
Hypertext Transfer/Transport Protocol (HTTP), 77, 104, 105
Hypertext Transfer/Transport Protocol Secure (HTTPS), 98, 209
hypervisors, 299

I

I2P (Invisible Internet Project), 100
IaaS (infrastructure as a service), 290–291
IBSS (Independent Basic Service Set), 325
ICSs (industrial control systems), 142
identification, incident response process, 397
identification of critical systems, 426
identity fraud, 16
identity theft, 22
IDS (intrusion detection system), 263–264
IEEE 802.1x authentication, 334–335
IEEE 802.11, 324
IEEE 802.11ac, 324
IEEE 802.11ax, 324
IEEE 802.11i, 334
IEEE 802.11n, 324
ifconfig (Linux), 237
image backup, 434
imaging utility, 411
IMAP (Internet Mail Access Protocol), 306
impact assessment, 468
impersonation, 16
implied trust constraint, 144
Impossible Travel, 438, 451
imprison, 67–69
  cryptomalware, 68–69
  ransomware, 67–68
improper input handling, 82
inability to patch constraint, 144
incident investigation, 402
  data sources, 402
    analyzers, 405
    IP monitors, 405
    log files, 402–405
    metadata, 405
    vulnerability scans, 405
  digital forensics, 405
    cloud forensics, 412–413
    procedures, 405–412
incident response, 400
  configuration changes, 402
  perform containment, 401–402
  SOAR runbooks and playbooks, 401
incident response plan, 397
incident response process, 397
incident response team, 397
incidents, 390–391
  access control
    Attribute-Based Access Control (ABAC), 396
    concepts, 391–392
    Discretionary Access Control (DAC), 394, 418–419
    Mandatory Access Control (MAC), 394–395
    Role-Based Access Control (RBAC), 395–396
    roles and terminology, 393
    Rule-Based Access Control, 396
    schemes, 392–396
    steps in, 392
  access control list (ACL), 396–397
  preparation
    creating an incident response plan, 397–398
    Cyber Kill Chain, 400
    Diamond Model of Intrusion Analysis, 399, 420
    MITRE ATT&Ck, 399
    performing exercises, 398
    studying attack frameworks, 399–400
  reasons for, 391–397
    poor access control, 391–397
    weak account types, 391
incremental backup, 434
Independent Basic Service Set (IBSS), 325
independent disks, with distributed parity, 430
indicator of compromise (IOC), 96
individual inconveniences, 467
individual theft, 467
industrial camouflage, 240
industrial control systems (ICSs), 142
industry-specific regulations, 52
influence campaigns, 15
information life cycle, 470
information security
  defining, 5–6
  hacktivists, 9
  insiders, 10
  layers, 6, 7
  script kiddies, 8–9
  state actors, 9–10
  understanding security, 5
  workforce, 4

Copyright 2022 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Information Security Community Site
  authentication, 387
  cloud computing, 315
  cyber incidents to law enforcement agencies, 421
  data privacy, 477
  social media analysis of posts, 452
  wireless network security, 348
information sources, 54
information technology (IT) assets, 455
infrared, 132
infrastructure as a service (IaaS), 290–291
infrastructure as code, 300–302
  software-defined network (SDN), 300–301
  software-defined visibility (SDV), 301–302
inherent risk, 462
initialization vector (IV), 331
injection attack, 78–79
inject malware, 330
inline system, 263
insider threat, 10
insurance companies, 459
integer overflow attack, 82
integrity, information security, 6
integrity measurement, 114
intellectual property (IP) theft, 456, 468, 476
intent/motivation, 8
interception attacks, 227
  man-in-the-browser (MITB), 228
  man-in-the-middle (MITM), 227
  session replay, 227–228
intermediate certificate authority (CA), 194
internal disasters, 425
internal physical security controls, 243
  fire suppression, 245
  locks, 243–244
  protected cable distribution, 244–245
  secure areas, 244
internal risk, 456
internal threat, actor, 8
International Organization for Standardization (ISO), 51
Internet Mail Access Protocol (IMAP), 306
Internet of Things (IoT), 143–144
Internet of Things (IoT) Cybersecurity Improvement Act of 2019, 145
Internet Protocol (IP) communications, 210
Internet Protocol Security (IPsec), 210
Internet Protocol version 6 (IPv6), 307, 315
intimidation, 15
intranet, 275
intrusion detection system (IDS), 263–264
intrusion prevention systems (IPS), 263–264
intrusive scans *vs.* nonintrusive scans, 46
invoice scam, 17
IOC (indicator of compromise), 96
IoT (Internet of Things), 143–145
IP (Internet Protocol)
  communications, 210
  network, 143
  schema, 265
ipconfig (Windows), 237
IPS (intrusion prevention systems), 263–264
IP (intellectual property) theft, 456, 468, 476
IPv6 (Internet Protocol version 6), 307, 315
iris, 366
ISO (International Organization for Standardization), 51
ISO 27001, 51
ISO 27002, 51
ISO 27701, 51
ISO 31000, 51
isolation, 402
IT (information technology) assets, 455
IT environment, security in, 5
IV (initialization vector), 331

J

jailbreaking, 136
jamming, 330
job rotation, 440
journalctl, log management tools, 404
jump box, 274, 275
jump host, 274
jump server, 274

K

Kali Linux penetration testing tool, 34
Kerberos, 375
key escrow, 206
key fob, 362
key handling procedures, 206–207
key length, 163
keylogger, 74–75
key management, 202
key risk indicators (KRIs), 96
key storage, 205
key stretching, 370–371
keystroke dynamics, authentication by, 368, 369, 383
key usage, 206
Kiosk OS, 109
knowledge-based authentication, 367
known ciphertext attack, 173
KRIs (key risk indicators), 96

L

L2TP (Layer 2 Tunneling Protocol), 267
lack of vendor support, 13
LAN (local area network), 132
laptop computer, 131
last known good configuration, 427
lateral movement, 41
launch attacks, 69
  bot, 72–73
  virus, 69–72
    file-based virus, 69–71
    fileless virus, 71–72
  worm, 72
law enforcement agencies, 459
layer 2 attacks, 228–230
  address resolution protocol poisoning, 229–230
  media access control attacks, 230–231
Layer 2 Tunneling Protocol (L2TP), 267
LDAP (Lightweight Directory Access Protocol), 306–307
LDAP injection attacks, 307
least privilege, 441
LED lights, 131
legacy BIOS boot, 103
legacy platforms, 11
legacy systems, 456
legal hold, 407
legislation, 53
lessons learned, incident response process, 397
level of capability, 8
lighting, 240
lightweight cryptography, 163
Lightweight Directory Access Protocol (LDAP), 306–307
likelihood of occurrence, 456
Linux file manipulation tools, 238
live boot media, 428
  nonpersistent, 428–449
living-off-the-land binaries (LOLBins), 71
load balancer, 275
load balancing, 275–276
local area network (LAN), 132
local management, cloud computing, 292
Local Security Policy, 449–450
location tracking, securing mobile devices, 135
lock, 243–244
  cable, 245
  electronic, 243
  physical, 243
lockout, 439
log, 47, 403
log files, 402–405
  collection and analysis tools, 420
  management tools, 404
  network device log sources, 403
  types of logs, 403
logic bomb, 76
log reviews, 47
LOLBins (living-off-the-land binaries), 71
longevity, 163
loop prevention, 270
low latency, 162
low-power devices, 162

M

MAC (Mandatory Access Control), 394–395
  elements to, 395
MAC (Media Access Control) address filtering, 332–333
MAC address spoofing, 271
MAC cloning attack, 231
MAC flooding attack, 231, 271
machine/computer digital certificate, 199
machine learning (ML), 84
  in cybersecurity, 85
macros, 71, 235
magnetic induction, 321
magnetic stripe cards, 362
malicious actor. *See* threat actor
malicious coding and scripting attacks, 234
  Bash, 236
  PowerShell, 234
  Python, 236
  visual basic for applications (VBA), 234–236
malicious flash drive, 135
malicious USB cable, 135

Copyright 2022 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

- malware (*mal*icious soft*ware*)
  - attacks using, 66–69
  - deceive, 75–76
    - potentially unwanted program (PUP), 75–76
    - remote access Trojan (RAT), 76
    - Trojan, 76
  - defining, 66
  - evade, 76–77
    - backdoor, 76
    - logic bomb, 76
    - rootkit, 76
  - imprison, 67–69
    - cryptomalware, 68–69
    - ransomware, 67–68
  - launch attacks, 69
    - bot, 72–73
    - virus, 69–72
    - worm, 72
  - snoop, 73–75
    - keylogger, 74–75
    - spyware, 73
- malware analysis reports (MARs), 99
- MAM (mobile application management), 139
- managed body sensor network (MBSN), 143
- managed security service provider (MSSP), 292
- managed service provider (MSP), 292
- managerial control, 461
- Mandatory Access Control (MAC), 394–395
- Mandatory Integrity Control (MIC), 395
- mandatory vacation, 440
- maneuvering, 49
- man-in-the-browser (MITB) attack, 228
- man-in-the-middle (MITM) attack, 227
- man-made disasters, 425
- mantrap, 244
- manual peer reviews, 116
- MARs (malware analysis reports), 99
- masking, 269
- Master Boot Record (MBR), 101
- MBR (Master Boot Record), 101
- MBSN (managed body sensor network), 143
- MCM (mobile content management), 139–140
- MD (message digest), 166
- MDM tools (mobile device management tools), 139
- mean time between failure (MTBF), 429, 458
- mean time to failure (MTTF), 458
- mean time to recovery (MTTR), 427
- Mean Time To Repair, 458
- measured boot, 103
- measurement system analysis (MSA), 463
- Media Access Control (MAC) address filtering, 332–333
- media access control attacks, 230–231
- media-based restore, 435
- memdump, 411
- memorandum of understanding (MOU), 463
- memory leak, 81
- memory management, 113
- memory vulnerabilities, 81–82
- mesh, 320
- message digest (MD), 166
- metadata, 405
  - entering and viewing, 417
- MFA (multifactor authentication), 361
- MFP (multifunctional printer), 143
- MIC (Mandatory Integrity Control), 395
- microphones, 135
- microprocessor, 5
- MicroSD HSM, 372
- microservices APIs, 294
- microservices architecture, 294
- Microsoft's Internet Information Services (IIS) web server, 113
- Microsoft version of CHAP (MS-CHAP), 377
- Microsoft Windows common LOLBins, 71
- mining cryptocurrencies, 73
- mirror image backup, 408
- mismatch scanning, 104
- mission-essential function, 426
- MITB attack (man-in-the-browser attack), 228
- mitigation, risk, 461
- MITM attack (man-in-the-middle attack), 227
- MITRE ATT&Ck, 399
- ML (machine learning), 84, 85
- MMS (multimedia messaging service), 136
- mobile application management (MAM), 139
- mobile computing device, 40
- mobile content management (MCM), 139–140
- mobile device location-based policies, 439
- mobile device management (MDM) tools, 139
- mobile devices, securing, 129
  - connectivity methods, 132
  - core and additional features, 129
  - enterprise deployment models, 133
  - location tracking, 135
  - physical security, 134
  - portable computers, 131–132
  - protecting mobile devices
    - device configuration, 136–139
    - mobile management tools, 139–140
  - risks, 134
    - accessing untrusted content, 135–136
    - enable loss or theft services, 138–139
    - mobile device connection vulnerabilities, 135
    - vulnerabilities, 134–135
  - security features for locating lost or stolen mobile devices, 139
  - smartphones, 130
  - tablets, 129–130
  - types, 129–132
  - unauthorized recording, 135
  - wearables, 130–131
- mobile management tools, 139–140
- mobile OS, 109
- mobile telecommunications switching office (MTSO), 132
- modern hardware and software platforms, 12
- moisture detection sensor, 243
- monitoring and response systems, 105–107
  - endpoint detection and response (EDR), 106–107
  - host intrusion detection system (HIDS), 105–106
  - host intrusion prevention system (HIPS), 106
- monitoring methodologies, 263–264
- monitoring services, 272
- monolithic architecture, 294
- motion detection sensor, 243
- motion recognition, 241
- MOU (memorandum of understanding), 463
- MSA (measurement system analysis), 463
- MS-CHAP (Microsoft version of CHAP), 377
- MSP (managed service provider), 292
- MSSP (managed security service provider), 292
- MTBF (mean time between failure), 429, 458
- MTSO (mobile telecommunications switching office), 132
- MTTF (mean time to failure), 458
- MTTR (mean time to recovery), 427
- multifactor authentication (MFA), 361
- multifunctional printer (MFP), 143
- multimedia messaging service (MMS), 136
- multiparty risks, 456, 476
- multipath, 431

N

- NAC (network access control), 267–268
- Narrowband Internet of Things (NB-IoT), 339
- NAS (network-attached storage), 435
  - devices, 423–424
- NAT (network address translation), 260
- National Institute of Standards and Technology (NIST), 50–51, 145
- National Security Agency (NSA), 110
- NB-IoT (Narrowband Internet of Things), 339
- NDA (nondisclosure agreement), 36, 441, 463
- near field communication (NFC), 321–322
- NERC standards (North American Electric Reliability Corp. standards), 52
- Nessus, 238
- Nessus hardware asset management, 44
- Nessus software asset management, 44
- NetFlow, 405
- .NET Framework, 71
- netsh commands, 346–347
- netstat (Windows, Linux), 237
- network, 431
- network access control (NAC), 267–268
- network address translation (NAT) gateway, 260
- network-attached storage (NAS), 435
  - devices, 423–424
- network constraint, 144
- network hardware security module, 264–265
- networking ACLs, 266
- network interface card (NIC), 431
- network intrusion detection system (NIDS), 264, 403
- network intrusion prevention system (NIPS), 264, 403
- network location, 438
- network OS, 109
- network segmentation, 272–275
- network sensors, 272
- network viruses. *See* worm
- network zones, 275

Copyright 2022 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

next generation firewall (NGFW), 261
NFC (near field communication), 321–322
NGFW (next generation firewall), 261
NIC (network interface card), 431
  teaming, 431
NIDS (network intrusion detection system), 264, 403
NIPS (network intrusion prevention system), 264, 403
NIST (National Institute of Standards and Technology), 50–51, 145
NIST Cybersecurity Framework (CSF), 51
NIST Risk Management Framework (RMF), 51
nmap, 238
nodal points, 367
noise detection sensor, 243
non-credentialed scans *vs.* credentialed scan, 45
nondisclosure agreement (NDA), 36, 441, 463
nonintrusive scans *vs.* intrusive scans, 46
nonpersistent, 428
  live boot Media, 428–449
  web browser, 475
nonrepudiation, 161
normalization, 116
North American Electric Reliability Corp. (NERC) standards, 52
North Ridge Security
  authentication, 387
  cloud computing, 315–316
  Firm and Fit (FAF), 476–477
  forensics investigations, 420–421
  Operating Appreciation, 452
  wireless network security, 348–349
NSA (National Security Agency), 110
nslookup (Windows), 237
nxlog, log management tools, 404

O

OAuth (Open Authorization), 373
obfuscation/camouflaged code, 116
object detection, 241
object identifier (OID), 205
Object Linking and Embedding (OLE) automation, 234
object, technical access control, 392
OCSP (Online Certificate Status Protocol), 195
OCSP Responder, 195
OCSP stapling, 196
offboarding, 441
off-boarding, risk, 464
Office of Management and Budget (OMB), 145
offline brute force attack, 358
offline CA, 194
offline uninterruptible power supply (UPS), 432
off-premises, 288
offsite backup, 435
OID (object identifier), 205
OLE automation (Object Linking and Embedding automation), 234
OMB (Office of Management and Budget), 145
onboarding, 441
on-boarding, risk, 464
on-body detection, 138
on demand, cloud computing, 288
one-time hash algorithms, digests generated from, 166
one-time pad (OTP), 164
one-time password (OTP), 362
online backup services, 451
online brute force attack, 358
online CA, 194
Online Certificate Status Protocol (OCSP), 195
online phishing training, 475
online restore, 435
online uninterruptible power supply (UPS), 432
on-prem and cloud, business continuity plan, 426
on-premises, 288
on-premises platforms, 12
onsite backup, 435
Opal, 177
Open ID, 373
open method, 333
open permissions, configurations, 13
open ports and services, 12
open source, 97
open source firewalls, 259
open source intelligence (OSINT), 40, 97
Open Source Interconnection (OSI) seven-layer model, 297
OpenSSL, 238
open systems interconnection (OSI) reference model, 228, 229
Open Web Application Security Project (OWASP), 115
Operating Appreciation, 452
operating systems (OSs), 108
  confinement tools, 110–111
  delays in patching, 14
  security configuration, 108–110
  types of, 109
  vulnerabilities in, 14
operational control, 461
operation, technical access control, 392
Opportunistic Wireless Encryption (OWE), 336
order of volatility, 407
original equipment manufacturer (OEM), 134
Orkney Islands, 285
OS event logs, 408
OSINT (open source intelligence), 40, 97
OSI reference model (open systems interconnection reference model), 228, 229
OSI (Open Source Interconnection) seven-layer model, 297
OSs. *See* operating systems (OSs)
OTP (one-time pad), 164
OTP (one-time password), 362
out-of-band management, 263
outsourced code development, 13
OWASP (Open Web Application Security Project), 115
OWE (Opportunistic Wireless Encryption), 336

P

.P7B, 201
.P12, 201
PaaS (platform as a service), 290, 412
packet capture and analysis, 271–272
packet capture and replay tools, 238–239
pagefile, 409
PAN (personal area network) technology, 319
PAP (Password Authentication Protocol), 377
passcode, authentication, 136–137
passive reconnaissance, 40
passive system, 263
passive tracking technologies, 73
pass the hash attack, 357
password, 355
  attacks on, 357–361
    brute force attack, 358
    dictionary attack, 359–360
    password collections, 360
    password spraying, 358
    rainbow tables, 360
    rule attack, 358–359
    tools, 361
  generators, 371
  Group Policy, 438
  management applications, 371, 386
  managing, 371–372
  online password cracker, 382
  protecting digests, 370–371
  requirements, 386
  security, 370–372
  vault, 371–372, 384
  weaknesses, 356–357
Password Authentication Protocol (PAP), 377
password collections attack, 360
password complexity, 438
password cracker, 358
password generators, 371
password history, 438
password keys, 372
password reuse, 438
password spraying attack, 358
password strength test, 386
patch distribution, 107
patch management, 107–108
patch reception, 107
pathping (Windows), 237
Patient Safety and Quality Improvement Act (PSQIA, Patient Safety Rule), 52
Payment Card Industry Data Security Standard (PCI DSS), 52, 272, 468
payment method, 321
pay-per-use, cloud computing, 288
PCI DSS (Payment Card Industry Data Security Standard), 52, 272, 468
PCI DSS Requirement 11 standards, 54
PCII (Protected Critical Infrastructure Information), 98
PDA (personal digital assistant), 132
PDU (power distribution unit), 431
PEAP (Protected EAP), 335
PEM (Privacy Enhancement Mail), 201
penetration testing (pen test)
  conducting, 35
  crowdsourced pen testers, 37
  defining, 34–35

Copyright 2022 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

  external pen tester consultants, 36
  levels, 37
  performance, 35, 39–40
    internal security personnel, 35–36
    penetration phase, 41–42
    reconnaissance phase, 40–41
  vs. vulnerability scan, 43
  war game teams, 35–36
percentage availability and downtimes, 426
perfect forward secrecy, 172
permanent NAC agent, 267
persistence, 40, 276
persistent, 428
personal area network (PAN) technology, 319
personal backup procedures, 451
personal digital assistant (PDA), 132
personal identification number (PIN), 136
Personal Information Exchange (PFX), 201
Personal Information Protection and Electronic Documents Act (PIPEDA), 52
Personally Identifiable Information (PII), 469
personal wireless security, 348
personnel policies
  acceptable use policy (AUP), 441–442
  clean desk space, 440
  data policies, 442–443
  job rotation, 440
  least privilege, 441
  mandatory vacation, 440
  onboarding and offboarding, 441
  organizational policies, 442
  separation of duties, 440
person-to-person contact, 16
PFIX (IP Flow Information Export), 405
pfSense open source firewall, 259
PFX (Personal Information Exchange), 201
pharming, 19
PHI (Protected Health Information), 469
phishing, 16–18
  spear, 17
phishing campaign, 465
phishing simulation, 465
phishing simulation dashboard, 465
phone call, 363
physical control, 462
physical locks, 243
physical security controls, 240
  computer hardware security, 245–246
  external perimeter defenses, 240
    barriers, 240–241
    personnel, 241–242
    sensors, 242–243
  internal physical security controls, 243
    fire suppression, 245
    locks, 243–244
    protected cable distribution, 244–245
    secure areas, 244
physiological biometrics, 365–367
picture password authentication, 368
PII (Personally Identifiable Information), 469
PIN (personal identification number), 136
ping (Windows, Linux), 237
pinning, 198
PIPEDA (Personal Information Protection and Electronic Documents Act), 52
pivot, 42
PKI. *See* public key infrastructure (PKI)
platform as a service (PaaS), 290, 412
platform/vendor-specific guides, 54
playbook, 401, 420
pointer/object dereference, 82
point-to-multipoint, 320
point-to-point, 320
policy, 436
  characteristics, 437
  types of security, 437–443
    account management policies, 437–439
    mobile device location-based policies, 439
    personnel policies, 439–443
POP (Post Office Protocol), 306
pop-up blocker, 104
portable computers, 131–132
port mirroring, 271
port security, 269–271
port spanning, 271
port TAP (test access point), 271
Post Office Protocol (POP), 306
post-quantum cryptography, 175
potentially unwanted program (PUP), 75–76
power, 431–432
power constraint, 144
power distribution unit (PDU), 431
PowerShell, 71, 234
predictive analysis, 96
preimage attack, 360
preparation, incident response process, 397
prepending technique, 16
preservation of the evidence, 406
preshared key (PSK), 333
pretexting, 16
preventative control, 462
privacy, 466–470
  data breach consequences, 468
  data destruction, 470
  data types, 468, 469
  protecting data, 468–470
  user concerns, 467
Privacy Enhancement Mail (PEM), 201
privacy notice, 468, 469, 476
private cloud, 288
private cluster connection, 428
private data, 469
private information sharing centers, 98
private key cryptography, 166
privileged access management, 393
privilege escalation, 41
process spawning control, 113
production stage, 114
Project 802, 324
Project Natick, 285–286
proper input validation, 116
proprietary data, 469
proprietary firewalls, 259
protected cable distribution, 244–245
Protected Critical Infrastructure Information (PCII), 98
Protected EAP (PEAP), 335
Protected Health Information (PHI), 469
protect endpoints, 103
  antimalware, 104
  antivirus, 103–104
  monitoring and response systems, 105–107
  web browsers, 104–105
protection, information security, 6
protocols, cryptographic, 207–208
  Hypertext Transport Protocol Secure (HTTPS), 209
  Internet Protocol Security (IPsec), 210
  Secure/Multipurpose Internet Mail Extensions (S/MIME), 209
  Secure Real-Time Transport Protocol (SRTP), 209
  Secure Shell (SSH), 208
  Secure Sockets Layer (SSL), 208
  Transport Layer Security (TLS), 208
  weaknesses of, 210
provenance, 407
provisioning, 114
proxies, 403
proximity sensor, 243
proxy servers, 261
  forward proxy, 261
  reverse proxy, 261
pseudo-anonymization, 469
PSK (preshared key), 333
PSQIA (Patient Safety and Quality Improvement Act), 52
public cloud, 288
public cluster connection, 428
public data, 469
public information sharing centers, 97
public key cryptography, 168, 192
public key infrastructure (PKI), 202
  key management, 205
    key handling procedures, 206–207
    key storage, 205
    key usage, 206
  management, 204–205
    certificate life cycle, 205
    certificate policy (CP), 204
    certificate practice statement (CPS), 204–205
  trust models, 202–204
    bridge trust model, 203–204
    distributed trust model, 203
    hierarchical trust model, 202–203
public notifications and disclosures, 468
pulping, 470
pulverizing, 470
PUP (potentially unwanted program), 75–76
purging, 470
purple team, penetration testing war game, 36
push notification, 363
push notification services, 139
Python, 236

Q

QA (quality assurance), 114
QoS (Quality of Service), 272
QR code (Quick Response code), 136
qualitative risk assessment, 458
quality assurance (QA), 114
Quality of Service (QoS), 272

Copyright 2022 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

quantitative risk assessment, 458
quantum communication, 174
quantum computer, 174
quantum cryptographic defenses, 174–175
quarantine, 111
Quick Response (QR) code, 136

R

race condition, 82
RACE Integrity Primitives Evaluation Message Digest, 166
radio frequency (RF), 132
radio frequency identification (RFID), 322–323
RADIUS (Remote Authentication Dial-In User Service), 374–376
RAID (Redundant Array of Inexpensive Disks), 428–430
rainbow tables, 360
RAM (random-access memory), 105
RAM slack, 409, 410
range constraint, 144
ransomware, 67–68, 423–424
  blocker, 67
  computer infection, 68
Raspberry Pi, 140, 141
RAT (remote access Trojan), 76
RBAC (Role-Based Access Control), 395–396
RB-RBAC (Rule-Based Role-Based Access Control) scheme, 396
RC (rivest cipher), 167
RCS (rich communication services), 136
RCSA (Risk Control Self-Assessment), 458
read wireless transmission, 330
real-time operating system (RTOS), 141
receptionist, 242
reconnaissance, 16, 40–41
  active, 40
  passive, 40
records retention policy, 443
recovery, incident response process, 397
recovery point objective (RPO), 433
recovery time objective (RTO), 433
Red Flags Rule, 52
redirection technique, 18–19
red team, penetration testing war game, 36
redundancy, 427
  resilience through, data, 433–436
refactoring, 83
reference architecture, 52
reference markers, 434
registration authority, 194
registry, 110
Regulation E (EFTA), 52
regulations, 52
  benchmark/secure configuration guides, 54
  broadly applicable, 52
  industry-specific, 52
  information sources, 54
  international, 52
  legislation, 53
  platform/vendor-specific guides, 54
  standards, 53–54
  U.S. state, 52
regulations that affect risk posture, 462
regulatory compliance, 53
regulatory/jurisdiction laws, 413
remote access Trojan (RAT), 76
remote access VPN, 267
Remote Authentication Dial-In User Service (RADIUS), 374–376
remote wipe, 138
removable media device, 14
replay attack, 80
replication, 428
reporting requirements/escalation, 398
reporting, rules of engagement, 39
reputation, 22
reputation damage, 468
request forgery, 80
  cross-site request forgery (CSRF), 80
  server-side request forgery (SSRF), 80
requests for comments (RFCs), 54
residual risk, 462
resilience, through redundancy
  data, 433–436
  disks, 428–431
  endpoints, 427–428
  networks, 431
  power, 431–432
  servers, 428
  sites, 433
resiliency, cloud computing, 288
resource policies, 292
resources and funding, 8
resource *vs.* security constraint, 162
response and recovery controls, 390
RESTful APIs, 294
restoration order, 427
retention policy, 398
retina, 365
reverse proxy, 261
revert to known state, 427
RF (radio frequency), 132
RFID (radio frequency identification), 322–323
rich communication services (RCS), 136
rights management, 268
right to audit clause, 412
RIPEMD, 166
risk awareness, 464
Risk Control Self-Assessment (RCSA), 458
Risk Management Framework (RMF), 51
risk matrix/heatmap, 459, 460
risk register, 459, 460
risks, 456
  analysis, 457–460
  assessment, 458–459
  decision-making biases and effects, 457–460
  defining, 455
  impact, 459
  likelihood, 458–459
  management, 461–466
    implement third-party risk management, 462–463
    provide user training, 464–466
    strategy, 461
    using controls, 461–462
  reacting to, 476
  representation, 459–460
  traits of learners, 464
  types, 456
Risky IP address, 438
rivest cipher (RC), 167
RMF (Risk Management Framework), 51
robot sentries, 242
rogue access point, 328
rogue AP system detection, 339–340
Role-Based Access Control (RBAC), 395–396
role-based awareness training, 465
roller barrier, 240
root digital certificates, 197–198
rooting, 136
rootkit, 76
rotating spikes, 240
route (Linux), 237
router ACLs, 266
routers and switches, 403
route security, 269–270
RPO (recovery point objective), 433
RSA, 169
rsyslog, log management tools, 404
RTO (recovery time objective), 433
RTOS (real-time operating system), 141
rule attack, 358–359
Rule-Based Access Control, 396
Rule-Based Role-Based Access Control (RB-RBAC) scheme, 396
rules of engagement, 37
  authorization, 38
  cleanup, 39
  communication, 39
  exploitation, 39
  reporting, 39
  scope, 38
  timing, 37
runbook, 401, 420
run-time verification, 116

S

SaaS (software as a service), 289–290, 412
SAE (Simultaneous Authentication of Equals), 336
safe, computer hardware security, 245
salt, 370
SAML (Security Assertion Markup Language), 376–377, 386
sandbox, 111, 112, 302
SAN digital certificate (subject alternative name digital certificate), 199
sanitizing, 78
SAN (storage area network), multipath, 431
SANS (SysAdmin, Audit, Network and Security Institute), 115
Sarbanes-Oxley Act of 2002 (Sarbox), 52, 468
SCADA (supervisory control and data acquisition), 142
scalability, 115
  cloud computing, 288
scalability, business continuity plan, 426
scan. *See specific types of scan*
scanless, 238
scarcity, 16
scatternet, 320
scheduling protocols, 275
scope, rules of engagement, 38
screen lock, authentication, 137
scripting attack, 78

Copyright 2022 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

scripting tools, 238
script kiddies, 8–9
SDN (software-defined network), 300–301
  controllers, 431
SDV (software-defined visibility), 301–302
SEAndroid, 395
SECaaS (Security as a Service), 291
SecDevOps, creating and deploying, 112–118
  application development concepts, 114–115
  application vulnerabilities, 112, 113
  code testing, 116–118
  directory traversal attack, 113
  secure coding techniques, 115, 116
secondary hard disk drives, 423
secret algorithms, 212
secrets management, 294
secrets management systems, 315
secure areas, 244
secure baseline configurations, 265
secure boot, 103
secure coding practices and techniques, 114
secure coding techniques, 115, 116
secure cookies, 104–105
secure email protocols, 306
Secure FTP (SFTP), 306
secure hash algorithm (SHA), 166
Secure/Multipurpose Internet Mail Extensions (S/MIME), 209
Secure Neighbor Discovery (SEND) protocol, 307
secure Network protocols, 304
  Domain Name System Security Extensions (DNSSEC), 304–305
  File Transfer Protocol (FTP), 305–306
  Internet Protocol version 6 (IPv6), 307
  Lightweight Directory Access Protocol (LDAP), 306–307
  secure email protocols, 306
  Simple network Management Protocol (SNMP), 304
  use cases, 307–308
Secure Real-time Transport Protocol (SRTP), 209
Secure Shell (SSH), 208
Secure Sockets Layer (SSL), 208
secure telecommunications, 174
securing endpoint computers, 101
  confirm boot integrity, 101–103
    boot security, 102–103
    Unified Extensible Firmware Interface (UEFI), 101–102
  harden endpoints, 107
    operating systems, 108–112
    patch management, 107
  protect endpoints, 103
    antimalware, 104
    antivirus, 103–104
    monitoring and response systems, 105–107
    web browsers, 104–105
securing mobile devices, 129
  connectivity methods, 132
  core and additional features, 129
  enterprise deployment models, 133
  location tracking, 135
  physical security, 134
  portable computers, 131–132
  protecting mobile devices
    device configuration, 136–139
    mobile management tools, 139–140
  risks, 134
    accessing untrusted content, 135–136
    enable loss or theft services, 138–139
    mobile device connection vulnerabilities, 135
    vulnerabilities, 134–135
  security features for locating lost or stolen mobile devices, 139
  smartphones, 130
  tablets, 129–130
  types, 129–132
  unauthorized recording, 135
  wearables, 130–131
security
  and convenience, 5, 6
  defining, 5
  in IT environment, 5
security administrator, 4
security appliances, 256
  configuration management, 265
  deception instruments, 261
    honeypot, 262
    sinkholes, 263
  firewalls, 257
    categories, 258–260
    functions, 257–258
    open source *vs.* proprietary, 259
    rule actions, 257
    specialized firewall appliances, 260–261
    stateful *vs.* stateless, 258–259
  intrusion detection and prevention systems, 263–264
  network hardware security modules, 264–265
  proxy servers, 261
Security as a Service (SECaaS), 291
Security Assertion Markup Language (SAML), 376–377, 386
security configuration, 108–110
security constraints
  for embedded systems, 144
  vs. resource, 162
security controls, 293–295
security control testing, 302
security guards, 241
security identifier (SID), 395
Security Information and Event Management (SIEM), 48–49, 296
security key, 364
security manager, 4
security of the ML algorithms, 85
Security Orchestration, Automation, and Response (SOAR), 49, 401
security positions categories, 4
security technician, 4
security technologies, 266
  access technologies, 266–269
    access control list (ACL), 266
    data loss prevention (DLP), 268–269
    network access control (NAC), 267–268
    virtual private network (VPN), 266–267
  design technologies, 272
    load balancing, 275–276
    network segmentation, 272–275
  technologies for monitoring and managing, 269–272
    file integrity monitors, 272
    monitoring services, 272
    packet capture and analysis, 271–272
    port security, 269–271
    quality of Service (QoS), 272
security template, 110
security through obscurity, 161
security virtual device solutions, 296–298
SEDs (self-encrypting drives), 177
segment storage, 138
self-encrypting drives (SEDs), 177
self-signed certificates, 197
SEND (Secure Neighbor Discovery) protocol, 307
sensitive data, 469
sensors, 242–23
sentiment analysis, 49
separation of duties, 440
serverless infrastructure, 289
server OS, 109
servers, 428
server-side execution and validation, 116
server-side request forgery (SSRF), 80
service account, 391
service attack, distributed denial of, 233–234
service-level agreement (SLA), 463
service providers, cloud computing, 292
services integration, 292
session cookie, 105
Session Initiation Protocol (SIP), 403
session replay attack, 227–228
sFlow, 405
SFTP (Secure FTP), 306
SHA (secure hash algorithm), 166
shadow IT, 10
shared account, 391
shimming, 83
short message service (SMS), 18, 136
  texts, 412
shoulder surfing, 21
shredding, 470
SID (security identifier), 395
sideloading, 136
SIEM (Security Information and Event Management), 48–49, 296
signage, 240
signature-based monitoring, 264
SIM card (subscriber identity module card), 339
Simple Mail Transfer Protocol (SMTP), 306
Simple Network Management Protocol (SNMP), 304
  management information base (MIB), 312–313
simulation, incident response exercises, 398
Simultaneous Authentication of Equals (SAE), 336
single-factor authentication, 361
Single Loss Expectancy (SLE), 459
single point of failure, 426
single sign-on (SSO), 373

Copyright 2022 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

sinkholes, 263
SIP (Session Initiation Protocol), 403
site risk assessment, 426
sites, resilience, 433
site survey, 337
site-to-site VPN, 267
skimming, 362
SLA (service-level agreement), 463
slack, 409
SLE (Single Loss Expectancy), 459
smart card, 361–362
smart meters, 141
  vs. analog meters, 142
smartphones, 130, 363–364
smart watch, 130
S/MIME (Secure/Multipurpose Internet Mail Extensions), 209
smishing, 18
SMS (short message service), 18, 136
  texts, 412
SMTP (Simple Mail Transfer Protocol), 306
sn1per, 238
snapshot, 302, 408, 434
SNMP (Simple Network Management Protocol), 304
  management information base (MIB), 312–313
SNMPv3, 304
snoop, 73–75
  keylogger, 74–75
  spyware, 73
SOAR (Security Orchestration, Automation, and Response), 49, 401
SoC (system on a chip), 141
social engineering, 15
  effectiveness, 15–16
social engineering attacks, 15
  impacts of attacks, 21–22
  physical procedures, 20
    dumpster diving, 20–21
    shoulder surfing, 21
    tailgating, 21
  psychological approaches
    hoaxes, 20
    impersonation, 16
    phishing, 16–18
    redirection, 18–19
    spam, 19–20
    watering hole attack, 20
  psychological principles, 15–20
social media, 15
social media analysis, 441
  of posts, 452
social media influence campaign, 15
Social Security number (SSN), 21
SOCs (System and Organization Controls), 51
software as a service (SaaS), 289–290, 412
software, attacks on, 81–83
  external software components, 83
  improper exception handling, 82
  memory vulnerabilities, 81–82
software compliance and licensing, 456
software-defined network (SDN), 300–301
  controllers, 431
software-defined visibility (SDV), 301–302
software digital certificates, 199–200
software diversity, 114
software firewall, 259
software noncompliance, 456
solid-state drives (SSDs), 131, 428–429
someone you know, 355
something you are, 355
something you can do, 355
something you exhibit, 355
something you have, 355
something you know, 355
somewhere you are, 355
sophistication, 8
spam, 19–20
spamming attack, 73
SPAN (Switch Port Analyzer), 271
spanning-tree protocol (STP), 270
spear phishing, 17
spim, 20
split MAC architecture, 326
split tunnel, 267
spreading malware attack, 73
spyware, 73
SQL (Structured Query Language), 78
SQL injection, 78
  statements, 79
SRTP (Secure Real-time Transport Protocol), 209
SSAE (Statements on Standards for Attestation Engagements), 51
SSAE SOC 2 Type II report, 51
SSAE SOC 2 Type III report, 51
SSDs (solid-state drives), 131, 428–429
SSH (Secure Shell), 208
SSL (Secure Sockets Layer), 208
SSL stripping, 208
SSN (Social Security number), 21
SSO (single sign-on), 373
SSRF (server-side request forgery), 80
staging stage, 114
stakeholder management, 398
standard naming conventions, 265
standards, 53–54
stapling, 196
state actors, 9–10
stateful packet filtering, 258
state laws, deviations in, 53
stateless packet filtering, 258
stateless protocol, 105
Statements on Standards for Attestation Engagements (SSAE), 51
static code, 362
  analysis, 116
statistical inferences, 467
steal data, 330
steganography, 159
  data hidden by, 159
storage area network (SAN), multipath, 431
storage segmentation, 138
stored procedure, 116
storing backups, 435–436
STP (spanning-tree protocol), 270
strategic counterintelligence, 410
strategic intelligence, 410
stream cipher, 164
string scanning, 104
striping, 429
Structured Query Language (SQL), 78
Structured Threat Information Expression (STIX), 98
subject alternative name (SAN) digital certificate, 199
subject, technical access control, 392
subnotebook computer, 131
supervisory control and data acquisition (SCADA), 142
supplicant requests, 335
supply chain, 15
swap file, 409
Switch Port Analyzer (SPAN), 271
symmetric cryptographic algorithms, 166–167
  digital signature algorithm (DSA), 170–171
  elliptic curve cryptography (ECC), 169–170
  key exchange, 171–172
  RSA, 169
symmetric server cluster, 428
SysAdmin, Audit, Network and Security Institute (SANS), 115
syslog, log management tools, 404
syslog-ng, log management tools, 404
System and Organization Controls (SOCs), 51
system integration, 13
system modifying software, 73
system on a chip (SoC), 141
system tampering, 113

T

tabletop, incident response exercises, 398
tablets, 129–130
TACACS+ (Terminal Access Control Access Control System+), 375–376
tactics, techniques, and procedures (TTPs), 97
tags, 406
tailgating, 21
Tailored Access Operations (TAO), 110
tainted training data for machine learning, 85
tamper-evident tape, 406
TAO (Tailored Access Operations), 110
TAXII (Trusted Automated Exchange of Intelligence Information), 98
TCG (Trusted Computing Group), 177
Tcpdump, 239
TCP/IP protocol, 66
Tcpreplay, 239
technical control, 461
temperature detection sensor, 243
Terminal Access Control Access Control System+ (TACACS+), 375–376
terms of agreement, 468
testing stage, 114
tethering, 135
theHarvester, 238
thin client, 289
third parties, 13
  app store, 136
  cookies, 105
  risk management, implementation, 462–463

Copyright 2022 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

solution, 293, 470
trust, 202
third-party updates, 107
threat
classifications, 455
insider, 10
management, 34
map, 99
threat actor, 7–8, 10
threat feeds, 49, 54
threat hunting, 49
threat intelligence sources, 96–100
categories of, 97–98
closed source information, 98
open source information, 97–98
dark web, 100
file and code repositories, 99
threat map, 99
vulnerability database, 99
3DES (triple data encryption standard), 167
thwarting attacks through port security, 271
time-based login, 438
time-based one-time password (TOTP), 362
time of check/time of use race condition, 82
time of day, 438
time offset, 410
time stamp, 410
timing, rules of engagement, 37
Title 21 of the Code of Federal Regulations (21 CFR Part 11) Electronic Records, 52
TLDs (top-level domains), 18
TLP (Traffic-Light Protocol), 98
TLS (Transport Layer Security), 208
tokenization, 269, 469
token key, 364
tokens, 362
top-level domains (TLDs), 18
Tor software, 100
TOTP (time-based one-time password), 362
TPM (Trusted Platform Module), 177–178
traceroute (Linux), 237
tracert (Windows), 237
tracking software, 73
Traffic-Light Protocol (TLP), 98
traits of learners, 464
transference, risk, 461
transit gateway, 289
Transport Layer Security (TLS), 208
transport mode encrypts, 210
triple-A, 392
triple data encryption standard (3DES), 167
Trojan, 76
True Blues, 467
trust, 16
Trusted Automated Exchange of Intelligence Information (TAXII), 98
trusted boot, 103
Trusted Computing Group (TCG), 177
trusted devices, 138
trusted face, 138
trusted places, 138
Trusted Platform Module (TPM), 177–178
trusted voice, 138
trust models, 202
public key infrastructure (PKI), 202
bridge trust model, 203–204
distributed trust model, 203
hierarchical trust model, 202–203
trustworthy email protocols/standards, 315
TTPs (tactics, techniques, and procedures), 97
tunnel mode encrypts, 210
two-factor authentication (2FA), 361
Twofish, 167
two-person integrity/control, 241
type I and II hypervisors, 299
typo squatting, 18

U

UAC (user account control), 395, 419–420
UAVs (unmanned aerial vehicles), 40, 143, 241
UCC (Unified Communications Certificate), 199
UEFI (Unified Extensible Firmware Interface), 101–102
UEFI native mode, 103
UEM (unified endpoint management), 140
unauthentication mode of operation, 213
unauthorized packet capturing, 271
unconscious human biases, 457, 476
UNetbootin screen, 449
Unified Communications Certificate (UCC), 199
unified endpoint management (UEM), 140
Unified Extensible Firmware Interface (UEFI), 101–102
unified threat management (UTM), 261
uniform resource locator (URL), 18
uninterruptible power supply (UPS), 432
universal access, 435
universal serial bus (USB) connectors, 132
unmanned aerial vehicles (UAVs), 40, 143, 241
unsecured root accounts, 12
unsecure protocols, 13
UPS (uninterruptible power supply), 432
urgency, 16
URL (uniform resource locator), 18
URL redirection, 231
USA Patriot Act of 2001, 52
USB hard drives, 423
USB On-the-Go (OTG), 135
U.S. Bureau of Labor Statistics (BLS) Occupational Outlook Handbook, 4
U.S. Cyber Command, 99
user account, 391
user account control (UAC), 395, 419–420
user awareness and training, 476
user behavior analysis, 48–49
user digital certificate, 197
U.S. state regulations, 52
UTM (unified threat management), 261

V

vault, 245
VBA (Visual Basic for Applications), 234–236
VDI (virtual desktop infrastructure), 133, 299
vectors
attack, 14–15
direct access, 14
vein, 366
vendors, 462
vendors management, 13
version control, 115
video cameras, 135
VIP (virtual IP), 276
virtual desktop infrastructure (VDI), 133, 299
virtual firewall, 259
virtual IP (VIP), 276
virtualization
advantages, 300
container, 299
defining, 298–299
infrastructure as code, 300–302
software-defined network (SDN), 300–301
software-defined visibility (SDV), 301–302
security, 302–303
type I and type II hypervisors, 299
virtual LANs (VLANs), 273, 300
virtual machine (VM), 297
loading, 314
from physical computer, 313–314
virtual machine escape protection, 302
virtual machine sprawl avoidance, 303
virtual network, 296
virtual private clouds (VPCs), 289
virtual private network (VPN), 266–267
vishing, 18
visitor log, 242
Vistumbler, 345–346
Visual Basic for Applications (VBA), 234–236
VLANs (virtual LANs), 273, 300
VM (virtual machine), 297
voice over IP (VoIP), 143
voice recognition, 366
VoIP (voice over IP), 143
VPCs (virtual private clouds), 289
VPN (virtual private network), 266–267
VPN concentrators, 403
vulnerabilities
attacks based on application, 113
configurations, 12–13
cybersecurity, 11
database, 99
defined, 11
feeds, 54
memory, 81–82
in OSs, 14
patches, 13–14
platforms, 11
cloud, 12
legacy, 11
on-premises, 12
third parties, 13
zero day, 14
vulnerability scan, 405
conducting, 43–45
technical constraints, 43
workflow interruptions, 43
defining, 42–43

Copyright 2022 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

vulnerability scan (*Continued*)
  examining results, 46
    accuracy, 47
    importance, 46–47
  vs. penetration test, 43
  types of, 45–46
  vulnerability information, 46

W

WAF (web application firewall), 260
walkthrough, incident response exercises, 398
war driving, 40
war flying, 40
"war game" scenario, 35–36
warm site, 433
waterfall model, 114
watering hole attack, 20
weak configurations, 12–13
weak defaults constraint, 144
weak encryption, 13
weak key, 163
wearable technology, 130–131
web application firewall (WAF), 260
web-based computer, 131
web browser certificate revocation procedures, 196
web browsers, 104–105
webcams, 135
web of trust model, 202
web servers, 403
WEP (Wired Equivalent Privacy), 331–332
whaling, 17–18
white box, penetration testing levels, 37
white hat hackers, 8
whitelisting, 110
white team, penetration testing war game, 36
Wi-Fi, 132, 323
Wi-Fi analyzer, 337
Wi-Fi direct, 325
Wi-Fi Protected Access (WPA), 333–334
Wi-Fi Protected Access 2 (WPA2), 334–335
Wi-Fi Protected Access 3 (WPA3), 336
  features, 348
Wi-Fi Protected Setup (WPS), 332
wildcard digital certificate, 199
wildcard scanning, 104
windowed tokens, 362–363
Windows file types, 70
Windows host-based firewall, 260
Windows Management Instrumentation (WMI), 71
Windows Picture Password, 367, 385
Windows slack, 418
WinHex, 411
wiping, 470
Wired Equivalent Privacy (WEP), 331–332
wireless access point placement, 337
wireless attacks
  Bluetooth, 319–321
  near field communication (NFC), 321–322
  radio frequency identification (RFID), 322–323
  wireless local area network (WLAN), 323–331
wireless device probe, 339
wireless LAN controller (WLC), 326–327
wireless local area network (WLAN), 132, 323–331
  access point, 325
    captive portal, 327
    fat *vs.* thin, 325–326
    standalone *vs.* controller, 326
  consumer attacks, 330–331
  enterprise attacks, 327–330
  hardware, 325
  MAC address filtering, 332–333
  security information with Vistumbler, 345–346
  standards, 324
  versions, 324
  vulnerabilities, 331–334
  Wi-Fi Protected Access (WPA), 333–334
  Wi-Fi Protected Setup (WPS), 332
  Wired Equivalent Privacy (WEP), 331–332
wireless monitor tool, 344–345
wireless network security, 348
  configuring access points, 346
  netsh commands, 346–347
  protections, 336–340
    configuration, 338–339
    installation, 337–338
    rogue AP system detection, 339–340
    specialized systems communications, 339
  solutions, 334–336
    Wi-Fi Protected Access 2 (WPA2), 334–335
    Wi-Fi Protected Access 3 (WPA3), 336
  wireless attacks
    Bluetooth, 319–321
    near field communication (NFC), 321–322
    radio frequency identification (RFID), 322–323
    wireless local area network (WLAN), 323–331
wireless NIC adapter, 40
wireless probe, 339
wireless security, personal, 348
Wireshark, 239
WLAN (wireless local area network), 132, 323–331
  access point, 325
    captive portal, 327
    fat *vs.* thin, 325–326
    standalone *vs.* controller, 326
  consumer attacks, 330–331
  enterprise attacks, 327–330
  hardware, 325
  MAC address filtering, 332–333
  security information with Vistumbler, 345–346
  standards, 324
  versions, 324
  vulnerabilities, 331–334
  Wi-Fi Protected Access (WPA), 333–334
  Wi-Fi Protected Setup (WPS), 332
  Wired Equivalent Privacy (WEP), 331–332
WLC (wireless LAN controller), 326–327
WMI (Windows Management Instrumentation), 71
workforce, information security, 4
workstation OS, 109
worm, 72
WPA (Wi-Fi Protected Access), 333–334
WPS (Wi-Fi Protected Setup), 332

X

X.509 file formats, 201
XaaS (anything as a service), 291–292
XML (eXtensible Markup Language), 79
XML injection, 79
XTACACS (Extended TACACS), 375

Z

zero day vulnerabilities, 14
zero trust, 273
Zigbee, 339
zombie. *See* bot

Copyright 2022 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.