

Index

2FA (two-factor authentication) fatigue, 780
3DES (Triple DES), 256–257
802.11 standards, 527

A

AAA model, access control
 accounting, 648, 649
 authentication, 645–646
 device authenticators, 654–655, 661
 factors, 649–650
 mutual, 662
 password policies, 652
 passwordless, 660
 passwords, 651–653
 service authentication, 661–662
 smartcards, 654
 authorization, 648, 649
 identification, 645–646
 identity establishment, 647–648
 MFA (multifactor authentication), 659
 objects, 646–647
 proofing, 647–648
 registration, 647–648
 subjects, 646–647
AAA services, 8–11
ABAC (attribute-based access control),
 686, 690
abstraction, 12
abuse case testing, 756
access abuses, 459
access control, 447, 643–644. *See also* AAA
 model; remote access
 answers to review questions, 1095–1097
 answers to written labs, 1127
 attacks, 703–719
 CIA Triad and, 331, 644–645
 CPTED (Crime Prevention Through
 Fundamental Design), 447
 lattice-based access controls, 338
 logical access, 644
 physical access, 644
 ZTA (zero-trust architecture), 702–703
access control matrix, 683
access control models
 ABAC (attribute-based access control),
 686, 690
 authorization mechanisms, 683–684
 comparison, 682–694
 DAC (discretionary access control), 685
 ACLs (access control lists), 686
 MAC (mandatory access control),
 686, 690–693
 nondiscretionary, 685, 687–694
 permissions and, 682
 privileges and, 683
 RBAC (role-based access control),
 685, 687–689
 TBAC, 688
 rights and, 682
 risk-based access control, 686, 693–694
 rule-based access control, 685, 689–690
 security policies, 685
access control vestibule, 475
access points, 540–541
accessibility, 7
account management reviews, 760–761
account revocation, 670
accountability, 6
accounting, AAA model and, 8, 11, 648, 649
ACLs (access control lists), 686
 firewalls, 841
ACS (cost of the safeguard), 77
active response, IDS (intrusion detection
 system), 833
active-active systems, 599–600
active-passive systems, 599–600
administrative controls, 81
administrative law, 154–155, 182–183

- administrative physical security controls, 449
- adware, 1016
- AES (Advanced Encryption Standard), 259
- Agile software development, 968–969
- AI (artificial intelligence), 855–856
- AIC Triad. *See* CIA Triad (confidentiality, integrity, availability)
- AICPA (American Institute of Certified Public Accountants), 733
- AIS (automated indicator sharing), 361
- ALE (annualized loss expectancy), 70, 71–72, 113, 136
- algorithms, cryptography, 231
- AMP (asymmetric multiprocessing), 382
- analog communications, 568
- analytic attacks, 306
- AND logical operator, 233
- Android mobile devices, 407–408
- anonymization, 212–214
- answers to review questions
 - access control, 1095–1097
 - application attacks, 1111–1113
 - asset security, 1068–1069
 - authentication, 1092–1095
 - BCP (business continuity planning), 1063–1065
 - communications, 1089–1092
 - compliance, 1065–1067
 - countermeasures, 1077–1082
 - cryptographic applications, 1072–1074
 - cryptography, 1070–1072
 - design, 1074–1077
 - DRP (disaster recovery planning), 1104–1106
 - ethics, 1106–1108
 - governance, 1056–1059
 - incident response, 1102–1104
 - investigations, 1106–1108
 - laws, 1065–1067
 - malicious code, 1111–1113
 - network architecture, 1085–1089
 - network attacks, 1089–1092
 - personnel security, 1059–1063
 - physical security, 1082–1085
 - PKI (public key infrastructure), 1072–1074
 - regulations, 1065–1067
 - risk management, 1059–1063
 - security assessment, 1097–1099
 - security models, 1074–1077
 - security operations, 1099–1101
 - software development, 1108–1110
 - symmetric key algorithms, 1070–1072
 - threats, 1077–1082
 - vulnerabilities, 1077–1082
- answers to written labs
 - access control, 1127
 - asset security, 1119
 - authentication, 1126–1127
 - BCP (business continuity planning), 1117–1118
 - communication, 1125–1126
 - compliance, 1118
 - countermeasures, 1121–1122
 - cryptography, 1119–1120
 - design principles, 1121
 - DRP (disaster recovery planning), 1130
 - ethics, 1131
 - governance, 1116
 - investigations, 1131
 - laws, 1118
 - network attacks, 1125–1126
 - networks, 1124
 - personnel security, 1116–1117
 - physical access, 1123
 - PKI (public key infrastructure), 1120
 - regulations, 1118
 - risk management, 1116–1117
 - security assessment, 1127–1128
 - security models, 1121
 - security operations, 1128–1129
 - software development, 1131
 - symmetric key algorithms, 1119–1120
 - testing, 1127–1128
 - threats, 1121–1122
 - vulnerabilities, 1121–1122
- antennas, 534–535
- antimalware, 838–839
- anycast technology, 569
- APIPA (Automatic Private IP Addressing), 621–622
- APIs (application programming interfaces), 321, 979–980
 - microservices, 397
 - testing, 379
- applets, 379

- application attacks, 1021–1024
 - answers to review questions, 1111–1113
- application cells, 406
- application containers, 406
- Application Layer (OSI Model), 494, 495, 496, 497
 - protocols, 503–504
- application logs, 844
- application security controls
 - code security, 1042–1044
 - database security, 1041
 - input validation, 1038–1039
 - WAFs (web application firewalls), 1040
- application-level firewalls, 553
- applied cryptography
 - blockchain, 304
 - email, 295–298
 - homomorphic encryption, 305
 - lightweight cryptography, 305
 - networking, 302–304
 - portable devices, 294–295
 - steganography, 300–302
 - TPM (Trusted Platform Module), 294
 - watermarking, 300–302
 - web applications, 298–300
- APTs (advanced persistent threat), 777, 1007
- ARO (annualized rate of occurrence), 70, 71, 113, 134
- ARP (Address Resolution Protocol), 506, 516–517
- Assets
 - classifications, 195
 - ownership, 781
- asset management, 781–783
- asset security
 - answers to review questions, 1068–1069
 - answers to written labs, 1119
 - compliance requirements, 196
 - data classifications, 192–195
 - data collection limitation, 202–203
 - data destruction, 205–207
 - data location, 203
 - data maintenance, 199
 - data protection, 209–214
 - data roles, 214–216
 - data security controls, 197–198
 - data states, 195–196
 - DLP (data loss prevention), 199–200, 220
 - end of support, 208
 - EOL (end of life), 208
 - handling information and assets, 201–202
 - labeling sensitive information, 200–201
 - record retention, 207
 - security control baseline, 216–219
 - sensitive data, 190–192
 - storing sensitive data, 203–204
- asset valuation, 61, 64–65
- asymmetric cryptography
 - Diffie-Hellman key exchange, 277–278
 - ECC (elliptic curve cryptography), 276–277
 - ElGamal, 275–276
 - key length, 275
 - key management, 292–293
 - Merkle-Hellman Knapsack, 274
 - private keys, 272–273
 - public keys, 272–273
 - quantum cryptography, 278–279
 - RSA (Rivest-Shamir-Adelman), 274
- asymmetric key algorithms, 250–253
- asynchronous communications, 569
- ATO (authorization to operate), 16, 348
- attacks, 62
 - applications, 1021–1024
 - botnets, 820–821
 - coding flaws and, 428–429
 - computer crime, 936–939
 - cryptographic, 306–309
 - design flaws and, 428–429
 - DoS (denial-of-service), 822–825
 - incremental attacks, 430–431
 - MAC flooding, 616
 - malware, 1006–1018
 - MiTM (man-in-the-middle), 827–828
 - MITRE ATT&CK, 857–858
 - ping floods, 825–826
 - sabotage, 828
 - salami attacks, 430–431
 - TCP reset, 824
 - wireless networks, 540–543
 - zero-day exploits, 826–827
- audit trails, 846
- auditing, AAA services, 8, 10
- AUP (acceptable use policy), 53–54
- authentication
 - AAA services, 8, 9–10, 649–653

- answers to review questions, 1092–1095
- answers to written labs, 1126–1127
- context-aware, 650
- device authenticators, 654–655, 661
- MFA (multifactor authentication), 11, 659
- microservices, 397
- mutual, 662
- passwordless, 660
- protocols, 582–584
- service authentication, 661–662
- smartcards, 654
- authentication system implementation
 - OAuth, 696, 697
 - OIDC (OpenID Connect), 696–697
 - SAML (Security Assertion Markup Language), 695–696, 697
 - SSO (single sign-on), 694
 - AAA protocols, 698
 - Kerberos, 698–700
 - RADIUS, 701
 - TACACS+, 701
 - XML (eXtensible Markup Language), 694
- authenticity, DAD Triad, 8
- authoritative passwords, 652–653
- authorization
 - AAA model and, 8, 10, 648, 649
 - access control matrix, 683
 - capability lists, 683
 - constrained interfaces, 683–684
 - content-dependent access controls, 684
 - context-dependent access controls, 684
 - implicit deny, 683
 - microservices, 397
 - need to know, 684
 - principle of least privilege, 684
 - separation of duties and responsibilities, 684
 - vulnerabilities, 1030–1033
- authorization to operate (ATO), 16
- AV (asset value), 69, 132
- availability, CIA Triad, 4, 6–7
- awareness, security training and, 106–107, 114
- background checks, 52
- backups, 901–904
- badges, 452–454
- baiting, social engineering, 101
- barricades, 476
- BAS (breach and attack simulation), 749
- baseband cables, 561
- baseband technology, 569
- baselines, 28
- bastion host, 552
- BC (business continuity), 122
- BCP (business continuity planning), 7, 122
 - answers to review questions, 1063–1065
 - answers to written labs, 1117–1118
 - BCP team selection, 124, 125–127, 146
 - benefits, 128
 - BIA (business impact analysis), 131–137
 - communication, training and education, 141
 - continuity planning, 137–140, 146
 - documentation, 141–146
 - versus* DRP (disaster recovery planning), 122–123
 - external dependencies, 124
 - legal requirements, 129–130, 146
 - organizational review, 123–125
 - plan approval, 140
 - plan implementation, 140–141
 - regulatory requirements, 129–130, 146
 - resource requirements, 124, 127–128
 - senior management and, 126–127
 - SLAs (service-level agreements), 130
 - vendors, 129
- BCP Development phase, 127
- BCP Implementation phase, 127
- BCP Testing, Training, and Maintenance phase, 127
- BEC (business email compromise), 97
- behavior modification, 106
- behavior-based intrusion detection, 830–831
- Bell-LaPadula model, 338–339
- BGP (Border Gateway Protocol), 499–500
- BIA (business impact analysis), 131, 146
 - disaster recovery and, 889–890
 - impact analysis, 135–137
 - likelihood assessment, 134–135
 - priority identification, 132–133
 - qualitative impact assessment, 131

B

- backbone distribution system, 451
- backdoors, 1023

- quantitative impact assessment, 131
- resource prioritization, 137
- risk identification, 133–134
- Biba model, 340–342
- biometrics, 656–659
- BIOS (basic input/output system), 377
- birthday attack, 308
- bit flipping, 755
- blacklisting, 840
- block cipher modes of operation
 - CBC (Cipher Block Chaining), 254
 - CCM (Counter with Cipher Block Chaining Message Authentication Code mode), 255–256
 - CFB (Cipher Feedback), 254–255
 - CTR (counter) mode, 255
 - ECB (Electronic Cookbook), 254
 - GCM (Galois/Counter mode), 255
 - OFB (Output Feedback), 255
- block ciphers, 246
- blockchain, 304
- Blowfish, 258
- Bluetooth, 537–538
- BMS (balanced magnetic switch), 456
- Boolean mathematics, cryptography, 232
- boot attestation, 378
- botnets, 1013
 - C&C/C2 (command-and-control) servers, 820
 - Mirai botnet, 821
 - sandboxing and, 821
 - users and, 821
- bottom-up approach, 17
- breaches, 62
- Brewer and Nash model, 343–344
- broadband cables, 561
- broadband technology, 569
- broadcast technology, 569
- brute-force attacks, 306
- BSoD (Blue Screen of Death), 325
- BSSID (basic service set identifier), 529
- buffer overflows, 1021–1022
- bus topology, 566
- business case, 17–18
- business continuity, 761
- business interruption, cybersecurity
 - insurance and, 76
- business strategy goals, 17–18

C

- C&C/C2 (command-and-control) servers, 820
- cable locks, 449
- cable plant management policy, 450–451
- cabling, 561–564
- CALEA (Communications Assistance for Law Enforcement Act), 169
- CAM (content addressable memory) table, 613
- cameras, 458–459
- Canadian privacy law, 176–177, 183–184
- candidate screening/hiring, 52–53
- capability lists, 683
- captive portals, 535
- carrier network connections, 627
- CASB (cloud access security broker), 210, 221
- CAST algorithms, 260
- casting technologies, 569
- CBC (Cipher Block Chaining), 254, 256
- CC (Common Criteria), 345–347
- CCE (Common Configuration Enumeration), 736
- CCM (Counter with Cipher Block Chaining Message Authentication Code mode), 255–256
- CCPA (California Consumer Privacy Act), 179
- CCTV (closed-circuit television), 458
- CDMA (Code Division Multiple Access), 537
- CDNs (content distribution networks), 544–545
- CEO spoofing, 97
- certificate pinning, 290
- certificate stapling, 291
- CFAA (Computer Fraud and Abuse Act), 153
- CFB (Cipher Feedback), 254–255, 256
- CFR (Code of Federal Regulations), 155
- change logs, 844
- change management, 793–796
- chat, 596–597
- Children's Online Privacy Protection Act (COPPA), 171
- Chinese privacy law, 177–178, 183–184
- chosen ciphertext attack, 308

- chosen plaintext attack, 308
- CIA Triad (confidentiality, integrity, availability), 4–7
 - access controls and, 331, 644–645
 - bounds and, 330–331
 - confinement and, 330
 - isolation and, 331
 - trust systems and, 331–332
- CIDR (Classless Inter-Domain Routing), 515
- CIO (chief information officer), 18
- ciphers
 - block ciphers, 246
 - versus* codes, 239
 - one-time pads, 243–244
 - running key ciphers, 244–245
 - stream ciphers, 246
 - substitution ciphers, 240–243
 - transposition ciphers, 239–240
- ciphertext, 231
- ciphertext-only attack, 307
- circuit encryption, 302–303
- circuit-level firewalls, 553–554, 841
- CIRT (cyber incident response team), 21, 814
- CIS (Center for Internet Security), 23
- CISO (chief information security officer), 18
- civil law, 154, 182–183
- Clarifying Lawful Overseas Use of Data (CLOUD) Act, 172–173
- Clark-Wilson model, 342–343
- clickjacking, 103
- client-based systems, vulnerabilities, 378–381
- clipping levels, 851
- closed source, 322
- closed systems, 321–322
- CLOUD (Clarifying Lawful Overseas Use of Data) Act, 172–173
- cloud services license agreements, 166
- cloud-based assets, 786
 - CSP (cloud service provider), 790
 - deployment models, 788
 - elasticity, 789–790
 - IaaS (infrastructure as a service), 788
 - PaaS (platform as a service), 788
 - SaaS (software as a service), 787
 - scalability, 789–790
 - serverless architecture, 790
 - services integration, 790
 - shared responsibility, 787–789
 - XaaS (anything as a service), 789
- cloud-based storage of symmetric keys, 262
- CM (configuration management), 790–793
- CMM (Capability Maturity Model), 86, 971–972
- CNC (covenant not to compete), 54
- coaxial cable, 561
- COBIT (Control Objectives for Information and Related Technologies), 15–16, 24, 735
- code injection attacks, 1028–1029
- code repositories, 981–982
- code security
 - application resilience, 1044
 - code repositories, 1043
 - code reuse, 1042–1043
 - code signing, 1042
 - comments, 1044
 - error handling, 1045–1046
 - hard-coded credentials, 1046–1047
 - integrity measurement, 1043
 - memory management, 1047–1048
 - software diversity, 1043
- cognitive passwords, 647
- collaboration. *See also* multimedia
 - collaboration
- collision attacks, 308
- collusion, 55
- combination locks, 478–479
- command injection attacks, 1029
- communications. *See also* multimedia
 - collaboration
 - answers to review questions, 1089–1092
 - answers to written labs, 1125–1126
 - emergency communication, 891
 - faxes, 605
 - protocols, 517–518
- Communications Assistance for Law Enforcement Act (CALEA), 169
- community cloud deployment model, 788
- compensating controls, 83–84
- compliance, 76–77, 179–181, 184
 - answers to review questions, 1065–1067
 - answers to written labs, 1118
 - requirements, 196
- computer crime, 183, 934
 - business attacks, 936

- CCCA (Comprehensive Crime Control Act), 156
- CFAA (Computer Fraud and Abuse Act), 156–157
- federal cybersecurity laws, 159–160
- financial attacks, 937
- FISMA (Federal Information Security Management Act), 158–159
- grudge attacks, 938–939
- hactivists, 940
- military and intelligence attacks, 935–936
- NIIPA (National Information Infrastructure Protection Act), 158
- terrorist attacks, 937
- thrill attacks, 939
- concealment, 5
- concurrent use licenses, 166
- conductors, cabling, 563
- confidential data, 192, 194
- confidentiality, CIA Triad, 4, 5
- consensus, social engineering, 93
- constrained interfaces, 683–684
- consultant agreements, 58–59
- container security, microservices, 397
- containerization, 406
- content filtering, 556
- content-dependent access controls, 684
- context-aware authentication, 650
- context-dependent access controls, 684
- continuity planning, 137–140
- continuous improvement, 86–87
- contractor agreements, 58–59
- contracts, 181–182, 184
- control zones, 375
- controls gap, 75
- converged protocols, 520–521
- COPPA (Children’s Online Privacy Protection Act), 171
- copyright law, 160–162, 183
- CORBA (Common Object Request Broker Architecture), 387
- corrective controls, 83
- COTS (commercial off-the-shelf), 983
- countermeasures, 62
 - answers to review questions, 1077–1082
 - answers to written labs, 1121–1122
 - implementing, 80–82
 - integrity, 6
 - physical controls, 82
 - selecting, 80–82
- covert channels, 427–428
- CPE (Common Platform Enumeration), 736
- CPTED (Crime Prevention Through Fundamental Design), 446–447
 - access control, 447
 - connectivity, 448
 - image, 447
 - milieu, 447–448
 - natural surveillance, 447
 - social cohesion, 448
 - territorial control, 448
 - threshold capacity, 448
- CPU (central processing unit)
 - execution types, 364–365
 - multicore, 364
 - multiprocessing, 365
 - multiprogramming, 365
 - multitasking, 364
 - multithreading, 365
 - protection mechanisms, 365–367
- credential hijacking, 102
- credential management systems, 666
- Credential Manager, 666–667
- crime. *See* computer crime
- criminal law, 152–154, 182–183
- criticality, 5
- cryptanalysis, 232
- cryptocurrency, 304
- cryptographic attacks, 306–309
- cryptographic erasure, 207
- cryptographic keys, 246–248
- cryptographic mathematics, 232–238
- cryptographic operations, 37
- cryptographic salt, 307
- cryptography
 - algorithms, 231
 - answers to review questions, 1070–1072
 - answers to written labs, 1119–1120
 - asymmetric, 272–279
 - key management, 292–293
 - asymmetric key algorithms, 250–253
 - authentication and, 230
 - ciphers, 239–246
 - ciphertext, 231
 - confidentiality and, 228–229
 - cryptanalysis, 232

- cryptographic keys, 246–248
- cryptology, 232
- cryptosystems, 232
- cryptovariables, 232
- DES (Data Encryption Standard), 248
- digital signatures, 283–286
- email, 295–298
- emerging applications, 304–305
- ephemeral key algorithms, 248–250
- FIPS (Federal Information Processing Standard), 232
- hash functions, 279–280
 - MD2 (Message Digest 2), 281
 - RIPEMD series, 282
 - SHA family, 280–281
 - value length comparison, 282–283
- hashing algorithms, 253
- hybrid, 293–294
- integrity and, 229–230
- Kerberos, 698–699
- Kerckhoff's principle, 231
- key spaces, 231
- life cycle, 263–264
- networking, 302–304
- nonrepudiation and, 230
- plaintext, 231, 246
- portable devices, 294–295
- private key algorithms, 248–250
- secret key algorithms, 248–250
- steganography, 300–302
- symmetric, 254–263
- symmetric key algorithms, 248–250
- watermarking, 300–302
- web applications, 298–300
- cryptology, 232
- cryptosystems, 232
- cryptovariables, 232
- CSF (Cybersecurity Framework), 23, 87, 88
- CSIRT (computer security incident response team), 814
- CSO (chief security officer), 18
- CSP (cloud service provider), 790
- CSR (certificate signing request), 289
- CSRF/XSRF (cross-site request forgery), 1036–1037
- CTR (counter) mode, 255, 256
- CUI (controlled unclassified information), 192

- CVE (Common Vulnerabilities and Exposures), 736
- dictionary, 800–801
- CVSS (Common Vulnerability Scoring System), 736
- CXL (Compute Express Link), 521
- cybersecurity insurance, 75–76

D

- DAC (discretionary access control), 685
 - ACLs (access control lists), 686
- DAD Triad, 7–8
- data at rest, 195
- data breaches, 75, 183
- data center controls, 452
- data classifications, 192–195
- data controllers, 215
- data custodians, 216
- data destruction, 220
 - clearing, 205–206
 - cryptographic erasure, 207
- data remanence
 - degaussers, 205
 - slack space, 204
 - SSDs, 205
- declassification, 206
- degaussing, 206
- destruction, 206
- erasing, 205
- overwriting, 205–206
- purging, 206
- data diddling, 430–431
- data exposure, 1041
- data hiding, 12–13
- data in transit, 195
- data in use, 195
- data localization, 362–363
- data minimization, 1041
- data owners, 214–215
- data processors, 215
- data protection
 - anonymization, 212–214
 - CASB (cloud access security broker), 210
 - DRM (digital rights management), 209
 - pseudonymization, 210–211
 - tokenization, 211–212

- data remanence, 374
- data remnants, 459
- data roles, 214–216, 221
- data security controls, 197–198
- data sovereignty, 361–363
- data states, 195–196, 220
- databases
 - recovery, 896–897
 - security, 1041
 - vulnerability scans, 745–746
- DBMS (database management system), 984
 - aggregation, 991–992
 - concurrency, 990–991
 - database transactions, 988–989
 - distributed data model, 985
 - hierarchical data model, 985
 - inference, 992
 - multilevel, 990–993
 - NoSQL databases, 994
 - ODBC (Open Database Connectivity), 993
 - relational databases, 985–988
 - storage, 994–995
- DCE (distributed computing environment),
 - vulnerabilities, 386–387
- DCOM (Distributed Component Object Model), 387
- DCSs (distributed control systems), 384–385
- DDoS (distributed denial-of-service)
 - attacks, 822
- declassification of data, 206
- decryption, 350
- deencapsulation, 494
- defense in breadth, 12
- defense in depth, 11–12
- degaussing, 206
- Delphi technique, 69
- DES (Data Encryption Standard), 248, 256
- design principles. *See also* security controls; security facility plan
 - answers to review questions, 1074–1077
 - answers to written labs, 1121
 - closed systems, 321–322
 - computing minimalism, 326
 - DRY (Don't Repeat Yourself), 326
 - failing securely, 323–325
 - KISS (keep it simple, stupid)
 - principle, 325–326
 - New Jersey Style, 326
 - objects, 319–320
 - open systems, 321–322
 - PbD (privacy by design), 328–329
 - rule of least power, 326
 - SASE (Secure Access Service Edge), 329–330
 - secure defaults, 322–323
 - security control implementation, 449–473
 - site selection, 445, 446
 - subjects, 319–320
 - trust but verify, 328
 - Worse is Better, 326
 - YAGNI (You Aren't Gonna Need It), 326
 - zero trust, 326–328
- detection, incident management,
 - 813–814, 818
- device authenticators, 654–655, 661
- DevOps, 977–978
- DHCP (Dynamic Host Configuration Protocol), 503
- DHSS (Direct Sequence Spread Spectrum), 536
- Diffie-Hellman key exchange, 277–278
- digital communications, 568
- digital signatures, 283–286
- digital watermarking, 853
- directive controls, 83
- DISA (direct inward system access), 591
- disaster recovery, 761
 - alternate processing sites, 891–896
 - availability, 883–889
 - BIA (business impact analysis), 889–890
 - crisis management and, 890
 - database recovery, 896–897
 - emergency communication, 891
 - fault tolerance, 883–889
 - system resilience, 883–889
 - workgroup recovery, 891
- disasters
 - earthquakes, 872–873
 - fires, 876–877
 - floods, 873–875
 - human-made, 877–883
 - natural disasters, 872
 - natural events, 877
 - pandemics, 877
 - storms, 875–876
- discretion, 5

- disinformation, 104
 - distance vector routing protocols, 499
 - diversity of defense, 12
 - DLP (data loss prevention), 199–200, 220, 853
 - DMCA (Digital Millennium Copyright Act), 160–162, 183
 - DMZ (demilitarized zone). *See* screened subnet
 - DNAT (destination network address translation), 619
 - DNP3 (Distributed Network Protocol 3), 520
 - DNS (Domain Name System), 506
 - ARP (Address Resolution Protocol), 506
 - domain hijacking, 511–512
 - IP addresses, 506
 - MAC addresses, 506
 - primary authoritative name server, 507
 - resource records, 507
 - secondary authoritative name server, 507
 - zone files, 507
 - DNS poisoning, 508
 - defenses, 510–511
 - DNS cache poisoning, 509
 - DNS pharming, 509
 - DNS query spoofing, 510
 - DNS sinkhole, 511
 - hosts file, 509–510
 - IP configuration corruption, 510
 - proxy falsification, 510
 - rogue DNS server, 509
 - split-DNS system, 510
 - DNSSEC (Domain Name System Security Extensions), 508
 - documentation
 - BCP (Business Continuity Planning), 141–145
 - change management and, 796
 - investigations, 934
 - documentation review, 16, 20
 - DoH (DNS over HTTPS), 508
 - domain hijacking, 511–512
 - domain name, 506
 - DoS (denial-of-service) attacks, 7, 31
 - DDoS (distributed denial-of-service), 822
 - DRDoS (distributed reflective denial-of-service), 823
 - exploitations, 822
 - Fraggle attacks, 824–825
 - Smurf attacks, 824–825
 - SYN flood attack, 823–824
 - doxing, 104
 - DPO (data privacy officer), 215
 - DR (disaster recovery), 122
 - DRDoS (distributed reflective denial-of-service) attacks, 823
 - DREAD (Damage, Reproducibility, Exploitability, Affected Users, and Discoverability) system, 34–35
 - DRM (digital rights management), 209–210, 221
 - DRP (disaster recovery planning), 132, 871, 898–899
 - answers to review questions, 1104–1106
 - answers to written labs, 1130
 - assessment, 900
 - awareness, 906–907
 - backups, 901–904
 - checklists, 900
 - communications, 900
 - documentation, 906–907
 - emergency response, 899
 - logistics, 905
 - personnel, 900
 - recovery *versus* restoration, 905–906
 - software escrow arrangement, 904–905
 - storage strategies, 901–903
 - supplies, 905
 - testing, 908–911
 - training, 906–907
 - utilities, 905
 - DSS (Digital Signature Standard), 285–286
 - due care, 27
 - due diligence, 27
 - dumpster diving, 102
 - duress systems, 778
 - DV (Domain Validation), 289
 - DWDM (Dense Wavelength Division Multiplexing), 564
 - dynamic ports, 505
-
- E**
- EALs (evaluation assurance levels), 346–347
 - EAP (Extensible Authentication Protocol), 533

- EAR (Export Administration Regulations), 167
 - eavesdropping, 630
 - ECB (Electronic Cookbook), 254, 256
 - ECC (elliptic curve cryptography), 276–277
 - Economic Espionage Act of 1996, 169, 183
 - ECPA (Electronic Communications Privacy Act), 153, 169
 - edge computing, 390–391
 - edge networks, 526
 - EDR (endpoint detection and response), 559
 - education, 107
 - EEPROM (electronically erasable programmable read-only memory), 369
 - EF (exposure factor), 70, 136
 - egress monitoring, 853
 - ELAs (Enterprise License Agreements), 166
 - elasticity, cloud-based assets, 789
 - Electronic Communications Privacy Act (ECPA), 169
 - elevation of privilege, 31
 - ElGamal, 275–276
 - email
 - data security, 197
 - encryption, 603–604
 - IMAP (Internet Message Access Protocol), 600
 - mail storms, 602
 - PGP (Pretty Good Privacy), 296–298
 - POP3 (Post Office Protocol version 3), 600
 - relays, 600
 - S/MIME, 298
 - security goals, 601–602
 - SMTP (Simple Mail Transfer Protocol), 600
 - spam, 98
 - spoofing, 602
 - emanation security, 374–376
 - emergency communication, 891
 - employee agreements, 53–54
 - employee oversight, 55, 112
 - employee transfers, 56, 112
 - EMSEC (Emission Security), 375
 - encapsulation, 494
 - encryption, 13, 350
 - email, 603–604
 - microservices, 397
 - endpoint security, 556–559
 - entrance facility, 450
 - environmental issues, 479
 - environmental monitoring, 466
 - EOL (end of life), devices, 87, 221
 - EOSL (end of service-life), devices, 87
 - EPA (Environmental Protection Agency), 446
 - ephemeral key algorithms, 248–250
 - ephemeral ports, 505
 - EPP (endpoint protection platform), 559
 - EPROM (erasable programmable read-only memory), 369
 - equipment failure, 450
 - equipment room, 451
 - erasing data, 205
 - ERM (enterprise risk management), 86
 - ESD (electrostatic discharge), 466
 - Ethernet, 568
 - ethics
 - answers to review questions, 1106–1108
 - answers to written labs, 1131
 - code of fair information practices, 944
 - ISC2 Code of Ethics, 941–942
 - organizational code, 940–941
 - RFC 1087, 943
 - Ten Commandments of Computer Ethics, 943
 - EU privacy law, 174–176, 183–184
 - EULAs (End-User License Agreements), 166
 - EV (Extended Validation), 289
 - evidence
 - artifacts, 926–930
 - chain of evidence, 924–925
 - forensic analysis, 928–930
 - hearsay rule, 925–926
 - Locard's exchange principle, 929
 - storage, 460–461
 - EVS (enhanced video surveillance), 458
 - exception handling, 323, 750
 - exclusive OR logical operator, 235
 - exercises, training, 758–759
 - exit interview, 57
 - extranets, 545
-
- F**
- FaaS (function as a service), 790
 - facility design, 446–448

facility security controls. *See* physical controls
 fail-open, 324, 960
 fail-safe, 324
 fail-secure system, 887–888, 960
 fail-soft, 324
 failing securely, 323–325
 failover clusters, 885–886
 familiarity, social engineering, 93
 Family Educational Rights and Privacy Act (FERPA), 173
 Faraday cage, 375
 fault injection attacks, 306
 fault tolerance, 350, 883–887
 FedRAMP, 25–26
 FERPA (Family Educational Rights and Privacy Act), 173
 FHSS (Frequency Hopping Spread Spectrum), 536
 fiber-optic cables, 564
 fiber-optic links, 629
 FIM (file integrity monitoring), 430
 financial loss protection, 75
 fire, 467–469
 damage, 473
 detection systems, 470–471
 extinguishers, 469–470
 fire detection systems, 470–471
 gas discharge systems, 472
 water suppression systems, 470–471
 firewalls, 551–555, 840–841
 ACLs and, 841
 application-level firewalls, 553
 circuit-level firewalls, 553–554, 841
 content filtering, 556
 directed broadcast blocking, 840
 distributed, 526
 ISFW (internal segmentation firewalls), 555
 logs, 844
 NGFW (next-generation firewall), 380, 554, 841
 private IP addresses blocking, 840–841
 proxy server, 555–556
 second-generation, 841
 stateful inspection firewalls, 554, 841
 static packet-filtering firewall, 553
 URL filtering, 556
 UTM (unified threat management), 841

 WAF (web application firewall), 380, 841, 1040
 firmware, 377–378
 flash memory, 369
 fog computing, 390–391
 forensic services, cybersecurity insurance and, 76
 FOUO (for official use only) data, 192
 FQDNs (fully qualified domain names), 507, 556
 Fraggie attacks, 824–825
 freeware licenses, 166
 FTP (File Transfer Protocol), 503
 full-duplex communication, 498
 fuzz testing, 30, 754–755

G

gait analysis, cameras, 458
 gamification, 108
 Gantt Charts, 975
 GCM (Galois/Counter mode), 255
 GDPR (General Data Protection Regulation), 155
 Generational (Intelligent) Fuzzing, 754
 GEO (geostationary orbit) satellites, 543
 geocast technology, 569
 GLB (greatest lower bound), 338
 governance, 14–16. *See also* security governance
 answers to review questions, 1056–1059
 answers to written labs, 1116
 GPOs (Group Policy Objects), 759
 GPS (Global Privacy Standard), 329
 Gramm-Leach-Bliley Act of 1999, 172

H

half-duplex communication, 498
 hardware
 asset inventories, 781–782
 CPU (central processing unit), 364–368
 data storage devices, 373–374
 emanation security, 374–376
 firmware, 377–378
 input/output devices, 376–377

- memory, 368
 - memory addressing, 371–372
 - RAM (random access memory), 369–371
 - registers, 371
 - ROM (read-only memory), 369
 - secondary memory, 372
 - networks, 546–549
 - hardware segmentation, 425–426
 - hardware-based storage of symmetric keys, 262
 - hash functions, 279–280
 - MD2 (Message Digest 2), 281
 - RIPEMD (RACE Integrity Primitives Evaluation Message Digest) series, 282
 - SHA (Secure Hash Algorithm)
 - SHA-1, 280
 - SHA-2, 280
 - SHA-3, 280
 - value length comparison, 282–283
 - hashing algorithms, 253, 1041
 - hazards, 63
 - Health Information Technology for Economic and Clinical Health (HITECH) Act, 170
 - HIDS (host-based IDS), 833–834
 - high availability, 883
 - HIPAA (Health Insurance Portability and Accountability Act), 170, 191
 - HITECH (Health Information Technology for Economic and Clinical Health) Act, 170
 - HMAC (Hash-Based Message Authentication Code), 284–285
 - hoaxes, 100
 - homograph attack, 512
 - homomorphic encryption, 305
 - honeynets, 836–837
 - honeypots, 836–837
 - hot and cold aisles, 465
 - HOTP (HMAC-based one-time passwords), 655
 - HPC (high-performance computing), 387–388
 - HR (human resources), 53
 - HSMs (hardware security modules), 293, 349–350
 - HTTP (Hypertext Transfer Protocol), 503
 - HTTPS (Hypertext Transfer Protocol Secure), 503
 - humidity, 464–466
 - hybrid cloud deployment model, 788
 - hybrid cryptography, 293–294
 - hybrid warfare, 105
-
- IaaS (infrastructure as a service), 403, 788
 - IaC (infrastructure as code), 397–398
 - IAM (identity and access management), 53
 - IANA (Internet Assigned Numbers Authority), 504, 841
 - IBoE (InfiniBand over Ethernet), 520
 - ICMP (Internet Control Message Protocol), 516
 - ICS (industrial control systems), vulnerabilities, 384–386
 - IDaaS (identity as a service), 666
 - IDE (integrated development environment), 955–956
 - IDEA (International Data Encryption Algorithm), 257–258
 - IDEAL model, 973–975
 - identification, AAA services, 8, 9
 - identity and access provisioning life cycle
 - account access review, 671–672
 - account maintenance, 671
 - account revocation, 670
 - enrollment, 668
 - offboarding, 670
 - onboarding, 668–670
 - roles, 670–671
 - identity fraud, 102–103
 - Identity Theft and Assumption Deterrence Act, 173
 - IDF (intermediate distribution frame), 451
 - IDL (interface definition language), 387
 - IdM (identity management)
 - centralized access, 662
 - credential management systems, 666
 - Credential Manager, 666–667
 - decentralized access, 663
 - LDAP directory, 663–664
 - scripted access, 667
 - session management, 667–668
 - SSO (single sign-on), 663–666
 - IDS (intrusion detection system), 454–455, 526, 828–829

- behavior-based detection, 830–831
- false alarms, 832
- HIDS (host-based IDS), 833–834
- intrusion alarms, 456–457
- knowledge-based detection, 829–830
- motion detectors, 455–456
- NIDS (network-based IDS), 833, 834–835
- perimeter breach detection, 456
- preventive controls
 - antimalware, 838–839
 - blacklisting, 840
 - firewalls, 840–841
 - honeynets, 836–837
 - honeypots, 836–837
 - sandboxing, 842
 - third-party security services, 842
 - warning banners, 837–838
 - whitelisting, 840
- response
 - active, 833
 - passive, 832–833
- secondary verification mechanisms, 457
- SIEM (security information and event management), 849–850
- signature-based detection, 832
- IETF (Internet Engineering Task Force), 325
- IGMP (Internet Group Management Protocol), 516
- IGRP (Interior Gateway Routing Protocol), 499
- IIoT (Industrial Internet of Things), 390
- IKE (Internet Key Exchange), 613
- IM (instant messaging), 596–597
- images for baselining, 791–792
- IMAP4 (Internet Message Access Protocol), 503
- immutable architecture, 398
- impersonation attacks, social engineering, 100, 704
- implementation attacks, 306
- implicit deny, 683
- import/export laws, 167–168
- incident management
 - attacks
 - botnets, 820–821
 - DoS (denial-of-service), 822–825
 - embedded systems, 821
 - IoT (Internet of Things), 821
 - MiTM (man-in-the-middle), 827–828
 - ping floods, 825–826
 - sabotage, 828
 - zero-day exploits, 826–827
 - CIRT (cyber incident response team), 814
 - computer security incident, 811
 - CSIRT (computer security incident response team), 814
 - detection, 813–814
 - detection controls, 818
 - IDPS (intrusion detection and prevention system), 828–829
 - IDS (intrusion detection system), 828–829
 - behavior-based detection, 830–831
 - false alarms, 832
 - knowledge-based detection, 829–830
 - response, 832–833
 - signature-based detection, 832
 - incident definition, 811–812
 - IPS (intrusion prevention system), 828–829
 - lessons learned, 817
 - log management, rollover logging, 852
 - logging techniques, 843–846
 - logs, 844–846, 850
 - mitigation, 814–815
 - monitoring
 - accountability and, 847
 - audit trails, 846
 - clipping levels, 851
 - egress monitoring, 853
 - investigations and, 848
 - keystroke monitoring, 851–852
 - network flow monitoring, 852
 - NTP (Network Time Protocol) and, 848
 - problem identification and, 848
 - sampling, 850–851
 - SIEM (security information and event management), 849–850
 - syslog, 850
 - traffic analysis, 852
 - trend analysis, 852
 - preventive controls, 818, 838–839
 - basic measures, 819
 - blacklisting, 840
 - firewalls, 840–841

- honeynets, 836–837
- honeypots, 836–837
- sandboxing, 842
- third-party security services, 842
- warning banners, 837–838
- whitelisting, 840
- recovery, 816
- remediation, 816–817
- reporting, 815–816
- response, 814
- tuning and, 848–849
- users, delegating to, 817–818
- incident response
 - AI (artificial intelligence), 855–856
 - answers to review questions, 1102–1104
 - answers to written labs, 1129
 - cybersecurity insurance and, 76
 - ML (machine learning), 855–856, 859
 - SOAR (security orchestration, automation, and response), 854–855, 859
 - threat feeds, 859
 - threat intelligence, 856–859
- incremental attacks, 430–431
- industrial camouflage, 446
- influence campaigns, 104–106
- information disclosure, 31
- information ownership, 781
- information system life cycle, 350–351
- InfoSec (information security) team, 18, 21
- inherent risk, 74
- injection vulnerabilities
 - code injection attacks, 1028–1029
 - command injection attacks, 1029
 - SQL injection attacks, 1024–1028
- input validation, 958, 1038–1039
- input/output devices, 376–377
- insider threats, 780
- intangible assets, 781
- intangible inventories, 782–783
- integrity, CIA Triad, 4, 6
- interfaces
 - constrained, 350
 - restricted, 350
 - testing, 755–756
- interior routing protocols, 499
- internal security, 478–479
- Internet files cache, 381
- intimidation, social engineering, 92–93
- intranets, 545
- intrusion alarms, 456–457
- investigations
 - administrative, 920–921
 - answers to review questions, 1106–1108
 - answers to written labs, 1131
 - civil, 921
 - conducting, 932–933
 - criminal, 921
 - data integrity and retention, 933–934
 - documentation, 934
 - electronic discovery, 922–923
 - evidence, 923–926
 - gathering, 930–931
 - industry standards and, 922
 - interviews, 933
 - law enforcement involvement, 931–932
 - operational, 920–921
 - regulatory, 922
 - reporting, 934
 - root cause analysis, 921
- invoice scams, 99
- iOS mobile devices, 408
- IoT (Internet of Things), 389–390
- IP (intellectual property)
 - copyright law, 160–162
 - DMCA (Digital Millennium Copyright Act), 160–162
 - patents, 163–164
 - trade secrets, 164–165
 - trademarks, 162–163
- IP (Internet Protocol), 512–516
- IP addresses, 506
- iPaaS (integration platform as a service), 790
- IPS (intrusion prevention system), 526, 836
 - NIPS (network-based IPS), 836
 - preventive controls
 - antimalware, 838–839
 - blacklisting, 840
 - firewalls, 840–841
 - honeynets, 836–837
 - honeypots, 836–837
 - sandboxing, 842
 - third-party security services, 842
 - warning banners, 837–838
 - whitelisting, 840
- SIEM (security information and event management), 849–850

IPSec (Internet Protocol Security), 518
 AH (Authentication Header), 612
 ESP (Encapsulating Security Payload), 612
 HMAC (Hash-based Message Authentication Code), 613
 IKE (Internet Key Exchange), 613
 IPComp (IP Payload Compression), 613
 VPNs, 612–613
 IPv4, addresses, 618–619
 IS (information systems), 3
 IS-IS (Intermediate system to Intermediate System), 499
 ISA (interconnection security agreement), 622
 ISC2 Code of Ethics, 941–942
 iSCSI (Internet Small Computer Systems Interface), 520
 ISFW (internal segmentation firewall), 327, 555
 ISO (information security officer), 18
 ISO (International Organization for Standardization), 23
 ISSID (independent service set identifier), 529
 IT (information technology), 3
 ITaaS (IT as a service), 403
 ITADA (Identity Theft and Assumption Deterrence Act), 153
 ITAR (International Traffic in Arms Regulations), 167
 ITIL (Information Technology Infrastructure Library), 26–27
 ITU (International Telecommunications Union), 629

J

Java applets, 379
 JavaScript, 380
 job rotation, 775

K

KBA (knowledge-based authentication), 647
 Kerberos, 518
 KDC (Key Distribution Center), 699
 login, 699–700
 TGT (ticket-granting ticket), 699

Kerckhoff's principle, cryptography, 231
 key spaces, 231
 keyboards/mice, 376
 keys, 478–479
 keystroke monitoring, 851–852
 kill chain, 856–857
 KISS (keep it simple, stupid)
 principle, 325–326
 knowledge-based intrusion
 detection, 829–830
 expert systems, 996–997
 ML (machine learning), 997
 neural networks, 997–998
 knowledge-based systems, 995
 known plaintext attack, 307
 KPIs (key performance indicators), physical security, 479–480

L

LAN media access, 570–572
 LAND attack, 826
 lattice-based access controls, 338
 laws
 administrative law, 154–155, 182–183
 answers to review questions, 1065–1067
 answers to written labs, 1118
 CFR (Code of Federal Regulations), 155
 civil law, 154, 182–183
 computer crime, 155–160, 183
 criminal law, 152–154, 182–183
 GDPR (General Data Protection Regulation), 155
 import/export, 167–168
 IP (intellectual property), 160–165
 privacy, 183–184
 Canadian privacy law, 176–177
 Chinese privacy law, 177–178
 EU privacy law, 174–176
 South African privacy law, 178–179
 state privacy laws, 179
 U.S. privacy law, 168–174
 software licensing, 166
 workplace, 174
 layering, 11–12

LDAP (Lightweight Directory Access Protocol), 663–664

LEAP (Lightweight Extensible Authentication Protocol), 531, 533, 583

legacy devices, 87, 114

legal liabilities, cybersecurity insurance and, 75

LEO (low Earth orbit) satellites, 543

lessons learned, incident management, 817

life cycle models, 965

- Agile software development, 968–969
- APIs (application programming interfaces), 979–980
- change management and, 976–977
- CMM (Capability Maturity Model), 971–972
- code repositories, 981–982
- configuration management and, 976–977
- DevOps approach, 977–978
- Gantt Charts, 975
- IDEAL model, 973–975
- PERT (Program Evaluation Review Technique), 975
- SAFe (Scaled Agile Framework), 970–971
- SAMM (Software Assurance Maturity Model), 972–973
- SDLC (software development life cycle), 965
- SLAs (service-level agreements), 982–983
- software testing, 980–981
- spiral model, 967
- third-party software acquisitions, 983–984
- waterfall model, 966–967

life safety, 479

link state routing protocols, 499

load balancing, 597–600

logic bombs, 1011–1012

logical access, 644

logical controls, 81

logical operations, cryptography

- AND, 233
- exclusive OR, 235
- modulo function, 235–236
- nonce, 236–237
- NOT, 234–235
- one-way functions, 236
- OR, 234

- split knowledge, 238
- work function, 238
- zero-knowledge proof, 237–238

logs

- analysis, 849
- application logs, 844
- change logs, 844
- data protection, 845–846
- firewall logs, 844
- log management, 852
- microservices, 397
- versus* monitoring, 10
- proxy logs, 844
- rollover logging, 852
- security logs, 844
- system logs, 844

logs reviews, 759–760

LPD (Line Printer Daemon), 503

LUB (least upper bound), 338

M

MaaS (monitoring as a service), 789

MAC (mandatory access control), 686, 690–693

MAC (Media Access Control) address, 500, 506

MAC cloning, 617

MAC spoofing, 617

magnetic stripe cards, 453

malicious code, 1007

- answers to review questions, 1111–1113

malicious scripts, 1017–1018

malware, 1006–1007

- adware, 1016
- antimalware software, 1019–1020
- EDR (endpoint detection and response), 1020–1021
- integrity monitoring, 1020
- logic bombs, 1011–1012
- malicious code, 1007
- malicious scripts, 1017–1018
- ransomware, 1016–1017
- spyware, 1016
- Trojan horses, 1012–1013

- UEBA (user and entity behavior analytics), 1021
- viruses, 1007–1011
- vulnerable platforms, 1019
- worms, 1013–1015
- zero-day attacks, 1018
- man-in-the-middle (MITM) attack, 308
- managed services, cloud-based, 786
 - elasticity, 789–790
 - scalability, 789–790
 - serverless architecture, 790
 - shared responsibility, 787–789
- mandatory vacations, 55, 112, 775
- masquerading, social engineering, 100
- MDF (main distribution frame), 451
- MDM (mobile device management)
 - systems, 650
 - ABAC models, 690
- MDR (managed detection and response), 559, 1021
- measured boot, 378
- media, installation media, 460
- media life cycle, 785
- media management, 783–785
- media storage facilities, 459–460
- meet-in-the-middle attack, 308
- memory, 368
 - memory addressing, 371–372
 - pagefiles, 372
 - RAM (random access memory), 369–371
 - registers, 371
 - ROM (read-only memory), 369
 - secondary memory, 372
 - swapfiles, 372
 - virtual memory, 372
- memory protection, 349
- MEO (medium Earth orbit) satellites, 543
- Merkle-Hellman Knapsack, 274
- mesh topology, 567
- metacharacters, 1039
- MFA (multifactor authentication), 11, 327, 659
- MFPs (multifunction printers), 376
- micro-training, 107
- microcontrollers, 392
- microservices, 396–397
- MIMO (Multiple Input, Multiple Output), 537
- Mirai botnet, 821
- mirroring, 884
- misinformation, 104
- misuse case testing, 756
- MiTM (man-in-the-middle) attack, 308, 827–828
- MITRE ATT&CK, 857–858
- ML (machine learning), 855–856, 997
- mobile devices, 407–408
 - Android, 407–408
 - deployment policies, 419–424
 - architecture and, 423
 - AUP (acceptable use policy), 423
 - BYOD (bring your own device), 420
 - COBO (corporate-owned, business-only), 421
 - COMS (corporate-owned mobile strategy), 421
 - contactless payment methods, 424
 - COPE (corporate-owned personally enabled), 420–421
 - CYOD (choose your own device), 420
 - data ownership and, 421
 - forensics, 422
 - hotspots, 424
 - infrastructure and, 423
 - legal concerns, 423
 - onboard camera/video, 423
 - patch management, 422
 - privacy, 422
 - QR (Quick Response) codes, 424
 - recording microphone, 423
 - security product management, 422
 - SIM cloning, 424
 - support ownership, 422
 - tethering, 424
 - update management, 422
- iOS, 408
- security features
 - application allow listing, 414
 - application control, 414
 - asset tracking, 416
 - carrier unlocking, 418
 - CMS (content management system), 414
 - communication protection, 410
 - credential management, 418–419
 - custom firmware, 418

- deactivating features, 416–417
- deny by default, 414
- device authentication, 409–410
- device lockout, 411–412
- FDE (full-device encryption), 410
- firmware over-the-air (OTA), 418
- geofencing, 413
- geolocation, 412
- geotagging, 412
- GPS, 412–413
- implicit deny, 414
- jailbreaking, 417
- location services, 412–413
- MAM (mobile application management), 414
- MCM (mobile content management), 414
- MDM (mobile device management), 409
- MMS (Multimedia Messaging Service), 419
- push notifications, 415
- RCS (Rich Communication Services), 419
- remote wiping, 411
- removable storage, 416
- rooting, 417
- screen locks, 411
- sideloading, 417–418
- SMS (Short Message Service), 419
- storage segmentation, 415–416
- text messaging, 419
- third-party app stores, 415
- VoIP and, 410
- modulo function, 235–236
- monitoring, 113
 - accountability and, 847
 - audit trails, 846
 - clipping levels, 851
 - egress monitoring, 853
 - investigations and, 848
 - keystroke monitoring, 851–852
 - log analysis, 849
 - versus* logs, 10
 - microservices, 397
 - network flow monitoring, 852
 - NTP (Network Time Protocol) and, 848
 - problem identification and, 848

- sampling, 850–851
- SIEM (security information and event management), 849–850
- traffic analysis, 852
- trend analysis, 852
- monitors, 376
- motion detectors, 455–456
- MOU (memorandum of understanding), 622
- MPP (massive parallel processing), 382–383
- MSPs (managed service providers), 403, 789
- MSSP (managed security service provider), 789
- MTBF (mean time between failures), 450, 786
- MTD (maximum tolerable downtime), 132
- MTO (maximum tolerable outage), 132
- MTTF (mean time to failure), 450, 785
- MTTR (mean time to repair), 450
- multicast technology, 569
- multimedia collaboration, 595–596
- multiparty risk, agreements and, 59
- multiplayer protocols, DNP3, 520
- Mutation (Dumb) Fuzzing, 754
- mutual authentication, 662

N

- NAC (network access control), 549–550
- named user licenses, 166
- NAPT (network address port translation), 619
- NAR (nuisance alarm rate), 474
- NAT (network address translation), 617–621
- NAT-T (NAT traversal), 619
- natural surveillance, 447
- NCA (non-compete agreement), 54
- NDA (nondisclosure agreement), 54
- need to know access control, 684
- network flow monitoring, 852
- network interfaces, testing, 756
- networks
 - 5-4-3- rule, 563
 - analog communications, 568
 - answers to review questions, 1085–1089
 - answers to written labs, 1124
 - asynchronous communications, 569
 - attacks

- answers to review questions, 1089–1092
 - answers to written labs, 1125–1126
 - eavesdropping, 630
 - modification attacks, 630–631
 - baseband technology, 569
 - broadband technology, 569
 - cabling, 561–564
 - casting technologies, 569
 - CDNs (content distribution networks), 544–545
 - cellular networks, 544
 - circuit encryption, 302–303
 - digital communications, 568
 - discovery scanning, 738–741
 - edge networks, 526
 - endpoint security, 556–559
 - Ethernet, 568
 - extranets, 545
 - firewalls, 551–556
 - hardware, 546–549
 - intranets, 545
 - IPSec, 303–304
 - LAN media access, 570–572
 - management, 597
 - mobile networks, 544
 - monitoring, 597
 - NAC (network access control), 549–550
 - physical address, 500
 - satellite communications, 543
 - screened hosts, 546
 - screened subnets, 545
 - sub-technologies, 568–572
 - synchronous communications, 569
 - topologies, 565–567
 - traffic, 502
 - transmission media, 560
 - transport architecture, 564–565
 - vulnerability scans, 741–743
 - wireless
 - 802.11 amendments, 527
 - antennas, 534–535
 - attacks, 539–543
 - captive portals, 535
 - channels, 529–530
 - general security procedure, 535–536
 - MAC filter, 534
 - security, 530–533
 - site surveys, 530
 - SSID security, 528–529
 - wireless communications, 536–539
 - WPS, 533
 - neural networks, 997–998
 - NFC (near-field communication), 539
 - NFS (Network File System), 504
 - NGFWs (next-generation firewalls), 380, 554, 841
 - NIDS (network-based IDS), 833, 834–835
 - NIPS (network-based IPS), 836
 - NIST (National Institute of Standards and Technology), 23
 - NOCs (network operations centers), IDSs and, 832–833
 - noise, 464
 - nonce, 236–237
 - nonrepudiation, DAD Triad, 8
 - NoSQL databases, 994
 - NOT logical operator, 234–235
 - NTP (Network Time Protocol), 759
 - monitoring and, 848
-
- O**
- OAuth, 696, 697
 - object-oriented programming. *See* OOP (object-oriented programming)
 - objects, design, 319–320
 - OCSP (Online Certificate Status Protocol), 289
 - ODBC (Open Database Connectivity), 993
 - OdoH (Oblivious DoH), 508
 - OFB (Output Feedback), 255, 256
 - OFDM (Orthogonal Frequency-Division Multiplexing), 536
 - off-the-shelf solutions, 361
 - OIDC (OpenID Connect), 696–697
 - on-site assessment, 20
 - onboarding employees, 112
 - AUP, 53–54
 - employee agreements, 53–54
 - IAM system, 53
 - principle of least privilege, 53
 - one-time pads, 243–244
 - one-way functions, 236
 - OOP (object-oriented programming), 12, 956–958
 - open source, 322

- open source licenses, 166
- open systems, 321–322
- operating states, 367–368
- operational plans, 19
- OR logical operator, 234
- organizational processes, security
 - governance, 19–21
- OS-virtualization, 406
- OSA (open system authentication), 531
- OSHA (Occupational Safety and Health Administration), 446
- OSI (Open Systems Interconnection), 493
- OSI Model, 493
 - Application Layer, 494, 495, 496, 497
 - protocols, 503–504
 - Data Link Layer, 495, 496, 500
 - deencapsulation, 494
 - encapsulation, 494
 - network container names, 496
 - Network Layer, 496, 498–500
 - peer-layer communication, 495
 - Physical Layer, 495, 496, 500–501
 - Presentation Layer, 496, 497
 - Session Layer, 496, 497–498
 - TCP/IP model comparison, 501
 - Transport Layer, 496, 498
 - protocols, 504–506
- OSPF (Open Shortest Path First), 499
- OSS (open source software), 983
- OT (operational technology), 384
- OTG (on-the-go), 416
- OTP (one-time password), 654–655
- outsourcing, 59
- OVAL (Open Vulnerability and Assessment Language), 736

P

- PaaS (platform as a service), 788
- pagefiles, 372
- PAM (privileged account management), 775–777
- parameter pollution, 1039
- passive response, IDS (intrusion detection system), 832–833
- passphrases, 651
- password attacks, 707
 - birthday attack, 711
 - brute-force attacks, 708–710
 - credential stuffing, 710
 - dictionary attacks, 708
 - Kerberos exploitation, 714–715
 - Mimikatz, 712–713
 - PtH (pass-the-hash), 713–714
 - rainbow table, 711–712
 - sniffer attack, 715–717
 - spraying attacks, 710
- passwordless authentication, 660
- passwords
 - authoritative, 652–653
 - cognitive passwords, 647
 - NIST recommendations, 653
 - OTP (one-time password), 654–655
 - PCI DSS requirements, 653
 - policies, 652
 - static, 651
 - vaults, 667
- PASTA (Process for Attack Simulation and Threat Analysis) threat model, 31
- PAT (port address translation), 619
- patch management, 797–798
- patents, 163–164, 183
- path vector, 499
- PBX (private branch exchange), 590–591
- PCI DSS (Payment Card Industry Data Security Standard), 25, 180–181
- PDSs (protective distribution systems), 451
- PEAP (Protected Extensible Authentication Protocol), 533, 583
- penetration testing, 3, 747–748
 - BAS (breach and attack simulation), 749
 - black-box penetration testing, 749
 - gray-box penetration testing, 749
 - white-box penetration testing, 749
- perimeter breach detection, 456
- perimeter security
 - access control vestibule, 475
 - barricades, 476
 - fences, 474
 - gates, 474
 - guard dogs, 477
 - lighting, 476–477
 - person trap, 475
 - robot sentries, 477
 - security bollards, 475–476

- security guards, 477
- turnstiles, 475
- permissions, access control and, 682
- perpetual licenses, 166
- person trap, 475
- personnel safety, 778–780
 - answers to review questions, 1059–1063
 - answers to written labs, 1116–1117
- personnel security policies and procedures
 - background checks, 52
 - candidate screening/hiring, 52–53
 - CNC (covenant not to compete), 54
 - consultant agreements, 58–59
 - contractor agreements, 58–59
 - employee oversight, 55
 - job descriptions, 51–52
 - job responsibilities, 52
 - NCA (non-compete agreement), 54
 - NDA (nondisclosure agreement), 54
 - offboarding, 56–57, 112
 - onboarding, 53–54
 - outsourcing and, 59
 - position description, 51–52
 - SLAs (service-level agreements), 59
 - vendor agreements, 58–59
 - VMS (vendor management system), 59–60
- PERT (Program Evaluation Review Technique), 975
- PFS (perfect forward secrecy), 300
- PGP (Pretty Good Privacy), 296–298
- PHI (protected health information), 170, 191, 220
- phishing, 95–96
 - whaling, 97–98
- phlashing, 378
- phreaking, 589–590
- physical access, 644
 - answers to review questions, 1082–1085
 - answers to written labs, 1123
- physical controls, 82, 449
 - access abuses, 459
 - badges, 452–454
 - cable plant management, 450–451
 - cameras, 458–459
 - data centers, 452
 - deciding on response, 449
 - delaying breaches, 449
 - denied access, 449
 - detecting intrusion, 449
 - determining causes, 449
 - deterred attempts, 449
 - environment monitoring, 466
 - equipment failure and, 450
 - ESD (electrostatic discharge), 466
 - evidence storage, 460–461
 - fire, 467–473
 - IDSs (intrusion detection systems), 454–457
 - internal security
 - combination locks, 478–479
 - environmental issues, 479
 - keys, 478–479
 - life safety, 479
 - regulatory requirements, 479
 - visitor logs, 478
 - KPIs (key performance indicators), 479–480
 - media storage facilities, 459–460
 - MTBF (mean time between failures), 450
 - MTTF (mean time to failure), 450
 - MTTR (mean time to repair), 450
 - perimeter, 474–477
 - proximity devices, 454
 - server rooms, 452
 - signage, 473
 - smartcards, 452–454
 - utilities
 - humidity, 464–466
 - noise, 464
 - power supply, 462–464
 - static, 464–466
 - temperature, 464–466
 - water issues, 467
 - wiring closets, 450–451
 - work area security, 461–462
- physical interfaces, testing, 756
- physical topology, 565
- PIDAS (perimeter intrusion detection and assessment system), 474
- piggybacking, 100–101
- PII (personally identifiable information), 190–191, 220
- ping floods, 825–826
- Ping-of-Death, 825
- PIPEDA (Personal Information Protection and Electronic Documents Act), 176–177
- PIPL (Personal Information Protection Law), 177–178

- PKI (public key infrastructure)
 - answers to review questions, 1072–1074
 - answers to written labs, 1120
 - CAs (certificate authorities), 287–288
 - certificate formats, 291–293
 - certificate lifecycle, 288–291
 - digital certificates, 286–287
- plaintext, 231
 - confusion and, 246
 - diffusion and, 246
- PLCs (programmable logic controllers), 384
- pointers, 372
- POP3 (Post Office Protocol), 503
- ports
 - dynamic, 505
 - ephemeral, 505
 - random, 505
 - registered software ports, 504
 - security, 585
 - service ports, 504
 - well-known ports, 504
- position description, 51–52
- POTS (plain old telephone service), 521
 - modems, 377
- power conditioners, 462
- power supply security, 462–464
- power-line conditioner, 462
- PPP (Point-to-Point Protocol), 582–583
- PPs (protection profiles), 346
- premises wire distribution room, 451
- preventive controls, incident
 - management, 82, 818
 - antimalware, 819, 838–839
 - applications, 819
 - blacklisting, 840
 - configuration management, 819
 - disabling services and protocols, 819
 - firewalls, 819, 840–841
 - honeynets, 836–837
 - honeypots, 836–837
 - IDS (intrusion detection system),
 - 454–457, 526, 819,
 - 828–835, 838–842
 - IPS (intrusion prevention system), 526,
 - 819, 836–842
 - removing services and protocols, 819
 - sandboxing, 842
 - system management, 819
 - systems, 819
 - third-party security services, 842
 - warning banners, 837–838
 - whitelisting, 840
- principle of least privilege, 53, 112, 684
 - privilege creep, 688
- printers, 376
- privacy, 5
- Privacy Act of 1974, 169
- privacy law, 183–184
 - Canada, 176–177
 - China, 177–178
 - EU, 174–176
 - South Africa, 178–179
 - states, 179
 - U.S., 168–174
 - workplace, 174
- private cloud deployment model, 788
- private data, 194
- private key algorithms, 248–250
- privilege creep, 688
- privilege escalation, 1023–1024
- privileges, access control and, 683
- proactive approach to threat
 - management, 30
- process isolation, 425
- process states
 - ready state, 367
 - running state, 368
 - stopped state, 368
 - supervisory state, 368
 - waiting state, 368
- process/policy review, 20
- procurement, 181–182, 184
- programming languages, 954–955
- PROM (programmable read-only
 - memory), 369
- promiscuous mode, 502
- propaganda, 104
- proprietary data, 194
- protection rings, 365–367
- protocol analyzers, 502
- protocols, 493
 - authentication protocols, 582–595
 - communication, 517–518
 - distance vector routing protocols, 499
 - FTP (File Transfer Protocol), 503
 - HTTP (Hypertext Transfer Protocol), 503

HTTPS (Hypertext Transfer Protocol Secure), 503
 ICMP (Internet Control Message Protocol), 516
 IGMP (Internet Group Management Protocol), 516
 IGRP (Interior Gateway Routing Protocol), 499
 IMAP4 (Internet Message Access Protocol), 503
 interior routing protocols, 499
 IP (Internet Protocol), 512–516
 legacy protocols, 499
 multilayer, 518–520
 converged protocols, 520–521
 DNP3, 520
 SDN (software-defined networking), 522–523
 VoIP (voice over IP), 521–522
 non-IP, 499
 OSI Model, 503–506
 POP3 (Post Office Protocol), 503
 port security, 585
 QoS (quality of service), 585–586
 routing protocols, 499–500
 S-RPC (Secure Remote Procedure Call), 518
 signal protocol, 518
 SMTP (Simple Mail Transfer Protocol), 503
 SNMP (Simple Network Management Protocol), 504
 SNMPv3, 504
 TCP (Transmission Control Protocol), 505
 TFTP (Trivial File Transfer Protocol), 503
 TLS (Transport Layer Security), 518
 proximity devices, 454
 proxy logs, 844
 proxy servers, 555
 pseudo-flaws, 837
 pseudonymization, 210–211, 221
 PSK (preshared key), 532
 PSTN (public switched telephone network), 521, 587
 PTZ (pan, tilt, and zoom), 458
 public cloud deployment model, 788
 public data, 194
 PUFs (physically unclonable functions), 36, 37
 purging data, 206

Q

QoS (quality of service), 585–586, 888
 qualitative impact assessment, BIA, 131
 qualitative risk analysis, 67, 68–69
 quantitative impact assessment, BIA, 131
 quantitative risk analysis, 67
 ALE (annualized loss expectancy), 70, 71–72
 ARO (annualized rate of occurrence), 70, 71
 AV (asset value), 69
 EF (exposure factor), 70
 formulas, 78–79
 hybrid assessment, 68
 SLE (single loss expectancy), 70, 71
 quantum cryptography, 278–279

R

RADIUS (Remote Authentication Dial-In User Service), 532–533, 701
 RAID array, 884–885
 random ports, 505
 ransomware, 1016–1017
 cybersecurity insurance and, 76
 RARP (Reverse Address Resolution Protocol), 835
 RATs (remote access Trojans), 1012
 RBAC (role-based access control), 685, 687–689
 TBAC (task-based access control), 688
 RC4 (Rivest Cipher 4), 259
 RC5 (Rivest Cipher 5), 259
 RC6 (Rivest Cipher 6), 259
 RDBMS (relational database management system), 984
 reactive approach to threat management, 30
 recovery. *See also* disaster recovery
 incident management, 816
 trusted recovery, 887–888
 recovery controls, 83
 reduction analysis, threat modeling and, 33
 registered software ports, 504
 regulatory compliance
 answers to review questions, 1065–1067

- answers to written labs, 1118
- cybersecurity insurance and, 76
- regulatory requirements, 479
- remanence, 374
- remediation, incident management, 816–817
- remote access
 - chat, 596–597
 - connection security, 592–593
 - IM (instant messaging), 596–597
 - network administrative functions, 594–595
 - remote node operation, 592
 - remote-control remote access, 592
 - security policies, 593–594
 - service-specific remote access, 592
 - telecommuting, 592
- remote attestation, 37
- replay attacks, 309
- reporting, incident management, 815–816
- repudiation, 31
- reputation, cybersecurity insurance and, 76
- request forgery, 1036–1037
- residual risk, 74
- resource protection, media management
 - protection techniques, 783–786
 - USB flash drives, 784
- response, incident management, 814
- responsibility, 6
- reverse hash matching, 308
- reviews, 109–110
- RFID (Radio Frequency Identification), 538–539
 - hardware asset inventory and, 782–783
- rights, access control and, 682
- ring topology, 565–566
- RIP (Routing Information Protocol), 499
- risk, 62
 - cyclical relationships, 63
- risk acceptance, 74
- risk assessment/analysis, 3, 60–61, 66–68, 112
 - qualitative risk analysis, 67
 - Delphi technique, 69
 - hybrid assessment, 68
 - scenarios, 68–69
 - quantitative risk analysis, 67, 78–79
 - ALE (annualized loss expectancy), 70, 71–72
 - ARO (annualized rate of occurrence), 70, 71
 - AV (asset value), 69
 - EF (exposure factor), 70
 - formulas, 78–79
 - hybrid assessment, 68
 - SLE (single loss expectancy), 70, 71
- scope, 67
- risk assignment, 74
- risk avoidance, 74
- risk awareness, 61
- risk deterrence, 74
- risk frameworks
 - CSF (Cybersecurity Framework), 87, 88
 - RMF (Risk Management Framework), 87, 88–90
- risk heat map, 86
- risk log, 85–86
- risk management, 60, 112
 - ACS (cost of the safeguard), 77
 - administrative controls, 81
 - answers to review questions, 1059–1063
 - answers to written labs, 1116–1117
 - asset valuation, 61, 64–65
 - assets and, 61
 - attacks, 62
 - breaches, 62
 - compliance, 76–77
 - continuous improvement
 - CMM (Capability Maturity Model), 86
 - ERM (enterprise risk management), 86
 - RMM (Risk Maturity Model), 86–87
 - cost/benefit evaluation, 76–79
 - countermeasures, 62
 - implementing, 80–82
 - selecting, 80–82
 - cybersecurity insurance, 75–76
 - exposure, 62
 - hazards, 63
 - IT infrastructure and, 60
 - legacy devices, 87
 - logical controls, 81
 - prioritization, 73
 - risk, 62
 - risk analysis, 60–61
 - risk assessment/analysis, 60–61, 66–73, 113
 - risk awareness, 61

- risk perspectives, 63–64
- risk reporting, 85–86
- safeguards, 62
- security controls, 62, 81–85
- technical controls, 81
- threat actors, 61
- threat agents, 61
- threat events, 62
- threat vectors, 62
- threats, 61
 - identifying, 65–66
 - vulnerabilities, 62, 65–66
- risk matrix, 86
- risk mitigation, 73
- risk register, 85
- risk rejection, 74
- risk reporting, 113
 - external reporting, 85
 - internal reporting, 85
 - risk heat map, 86
 - risk log, 85–86
 - risk matrix, 86
 - risk register, 85
- risk response, 61, 74–75
- risk-based access control, 686, 693–694
- Rivest Ciphers (RC), 258
 - RC4 (Rivest Cipher 4), 259
 - RC5 (Rivest Cipher 5), 259
 - RC6 (Rivest Cipher 6), 259
- RMF (Risk Management Framework), 23, 87, 88–90
 - ATO (authorization to operate), 348
- RMM (Risk Maturity Model), 86–87, 114
- ROI (return on investment), 19
- rollover logging, 852
- ROM (read-only memory), 369
- rootkits, 429–430, 1023–1024
- RoT (root of trust), 426
- RoT (silicon Root of Trust), 36–37
- routers, 499
- routing protocols, 499–500
 - BGP, 499–500
 - distance vector routing protocols, 499
 - IGRP (Interior Gateway Routing Protocol), 499
 - interior routing protocols, 499
 - IS-IS (Intermediate system to Intermediate System), 499

- link state routing protocols, 499
- OSPF (Open Shortest Path First), 499
- path vector, 499
- RIP (Routing Information Protocol), 499
- RPCs (remote procedure calls), 387
- RPO (recovery point objective), 133
- RSA (Rivest-Shamir-Adelman) algorithm, 274
- RTBH (remote triggered black hole), 552
- RTO (recovery time objective), 133
- RTOS (real-time OS), 388–389
- RTP (Real-Time Transport Protocol), 522
- rule-based access control, 685, 689–690
- RUM (real user monitoring), 757
- running key ciphers, 244–245
- runtime environments, 954

S

- S-RPC (Secure Remote Procedure Call), 518
- S/MIME (Secure/Multipurpose Internet Mail Extensions), 298
- SaaS (software as a service), 787
- sabotage, 828
- SABSA (Sherwood Applied Business Security Architecture), 24
- SAE (Simultaneous Authentication of Equals), 532
- SAFe (Scaled Agile Framework), 970–971
- safeguards, 62, 113
- salami attacks, 430–431
- SAML (Security Assertion Markup Language), 695–696, 697
- SAMM (Software Assurance Maturity Model), 972–973
- sampling, 850–851
- sandboxing, 842
 - botnets and, 821
- SANs (storage area network), 398, 520
- Sarbanes-Oxley Act (SOX), 181
- satellite communications, 543
- SBOM (software bill of materials), 36, 37
- SBU (sensitive but unclassified) data, 192
- SCA (security control assessment), 84, 113
- SCADA (supervisory control and data acquisition), 384
- scalability, cloud-based assets, 789

- SCAP (Security Content Automation Protocol), 736
- scarcity, social engineering, 93
- SCM (software configuration management), 977
- scope, 67
- screened hosts, 546
- screened subnets, 545
- script kiddies, 1007
- SCRM (supply chain risk management), 35
 - PUFs (physically unclonable functions), 36
 - RoT (silicon Root of Trust), 36–37
 - SBOM (software bill of materials), 36
- SD-WAN (software-defined wide area network), 690
- SDDC (software-defined data center), 403
- SDH (Synchronous Digital Hierarchy), 629
- SDLC (software development life cycle), 328
- SDN (software-defined networking), 398, 522–523
 - ABAC models, 690
- SDP (service delivery platform), 545
- SDS (software-defined storage), 523
- SDV (software-defined visibility), 403
- SDWAN (software-defined wide-area network), 523
- SDx (software-defined everything), 402–404
- SECaaS (security as a service), 789
- seclusion, 5
- secondary verification mechanisms, 457
- secrecy, 5
- secret data, 192
- secret key algorithms, 248–250
- secure boot, 37, 378
- secure facility plan, 444–448
- security, 3
 - classification levels, 339
 - data security controls, 197–198
 - legally defensible, 4
- security assessments, 731. *See also* vulnerability assessment
 - answers to review questions, 1097–1099
 - answers to written labs, 1127–1128
 - audits, 732–735
 - NIST (SP 800-53A), 731
 - penetration testing, 747–749
- security audits, 732
 - COBIT (Control Objectives for Information and Related Technologies), 735
 - external, 733
 - FAA (Federal Aviation Administration), 732
 - internal, 733
 - SOC (system and organization controls), 734
 - standards, 735
 - third-party, 733–735
- security awareness training and education, 107
- effectiveness evaluation, 110
- improving, 108
- micro-training, 107
- security baselines, 28
- security bollards, 475–476
- security boundaries, 13–14
- security champions, 108
- security control baseline, 216–219, 221
- security control frameworks, 22–23
 - COBIT (Control Objectives for Information and Related Technologies), 24
 - FedRAMP, 25–26
 - ISO (International Organization for Standardization), 23
 - ITIL (Information Technology Infrastructure Library), 26–27
 - NIST (National Institute of Standards and Technology), 23
 - PCI DSS (Payment Card Industry Data Security Standard), 25
 - SABSA (Sherwood Applied Business Security Architecture), 24
- security controls, 62
 - administrative controls, 81
 - compensating controls, 83–84
 - corrective controls, 83
 - detection controls, 82
 - deterrent controls, 83
 - directive controls, 83
 - logical controls, 81
 - measurement, 84–85
 - monitoring, 84–85
 - physical controls, 82, 449
 - preventive controls, 82

- recovery controls, 83
- SCA (security control assessment), 84
- technical controls, 81
- security facility plan, facility design,
 - CPTED (Crime Prevention Through Fundamental Design), 446–448
- security function, 16
 - business strategy goals and, 17–18
- security governance, 14
 - asset owner, 22
 - auditors, 22
 - custodian, 22
 - documentation review, 16
 - organizational processes, 19–21
 - security management planning, 17–19
 - security policies, 17
 - security professionals, 21
 - security roles, 21
 - senior manager, 21
 - SLR (service-level requirement), 21
 - users, 22
- security guidelines, 28
- security logs, 844
- security management
 - account management reviews, 760–761
 - business continuity, 761
 - disaster recovery, 761
 - key performance, 762
 - log reviews, 759–760
 - planning, 17–19
 - risk indicators, 762
 - training and awareness programs, 761
- security models
 - access control matrix, 337–338
 - answers to written labs, 1121
 - Bell-LaPadula model, 338–340
 - Biba model, 340–342
 - Brewer and Nash model, 343–344
 - capabilities, 332
 - Clark-Wilson model, 342–343
 - composition theories, 336
 - directed graphs, 336–337
 - FSM (finite state machine), 334–335
 - information flow model, 335
 - labels, 332
 - noninterference model, 335
 - star, 344
 - state machine model, 334–335
 - take-grant model, 336–337
 - TCB (trusted computing base), 333–334
 - tokens, 332
- security of assets. *See* asset security
- security operations, 771
 - answers to review questions, 1099–1101
 - answers to written labs, 1128–1129
 - APTs (advanced persistent threat), 777
 - job rotation, 775
 - least privilege principle, 772–773
 - mandatory vacations, 775
 - need-to-know access, 772
 - PAM (privileged account management), 775–777
 - SLAs (service-level agreements), 777
 - SoD (segregation of duties), 773–774
 - two-person control, 774
- security policies, 17–18, 28
 - access control, 685
- security questions, 647
- security standards, 28
- security testing, 729
 - ethical disclosure, 753
 - reviewing, 730
- security through obscurity, 5, 13
- Security Triad. *See* CIA Triad (confidentiality, integrity, availability)
- segmentation, 523
 - air-gapped, 524
 - distributed firewalls, 526
 - logical, 524
 - microsegmentation, 525
 - network overlays/encapsulation, 525–526
 - physical, 524
 - VLANs, 524
 - VPCs, 525
 - VPNs, 524–525
- senior management, 18
 - BCP and, 126–127
- sensitive data, 194, 220
- sensitivity, 5
- separation of duties and responsibilities, 684
- serial configuration, 11–12
- server room controls, 452
- server sprawl, 405
- server-based systems, vulnerabilities, 381
 - data flow control, 381

- grid computing, 383–384
- load balancers, 382
- P2P (peer-to-peer) technologies, 384
- parallel data systems, large scale, 382–383
- serverless architecture, 790
- service authentication, 661–662
- service ports, 504
- session hijacking, 1037
- SHA-3 (Secure Hash Algorithm 3), 853
- shadow IT, 210, 405
- shared responsibility, 360–361
 - cloud service models and, 787–789
- shielding cables, 376
- shoulder surfing, 99
- side-channel attacks, 306
- SIEM (security information and event management), 849–850
- signal protocol, 518
- signature-based intrusion detection, 832
- simplex communication, 498
- site security controls. *See* physical controls
- site selection, 445–447
- SKA (shared key authentication), 531
- SKIPJACK, 258
- SLAAC (Stateless Address
 - Autoconfiguration), 513
- SLAs (service-level agreements),
 - 59, 777, 982–983
 - BCP and, 130
- SLE (single loss expectancy), 70, 71, 113, 136
- SLR (service-level requirement), 21
- smartcards, 452–454, 654
- smishing, 96
- SMP (symmetric multiprocessing), 382
- SMS (Short Message Service), smishing, 96
- SMTP (Simple Mail Transfer Protocol), 503
- Smurf attacks, 824–825
- SNAT (Source Network Address
 - Translation), 619
- SNMP (Simple Network Management
 - Protocol), 504
 - SNMPv3, 504
- SOA (service-oriented architecture), 396
- SOAR (security orchestration, automation,
 - and response)
 - playbooks, 854–855
 - runbooks, 854–855
- SOC (system and organization controls), 734
- SoC (system on a chip), 549
- social engineering, 90, 114
 - authority, 92
 - baiting, 101
 - CEO spoofing, 97
 - clickjacking, 103
 - consensus, 93
 - credential hijacking, 102
 - dumpster diving, 102
 - eliciting information, 94
 - examples, 91
 - familiarity, 93
 - hoaxes, 100
 - identity fraud, 102–103
 - impersonation, 100
 - influence campaigns, 104–106
 - intimidation, 92–93
 - invoice scams, 99
 - masquerading, 100
 - phishing, 95–96
 - whaling, 97–98
 - piggybacking, 100–101
 - prepending, 94–95
 - protecting against, 91–92
 - scarcity, 93
 - shoulder surfing, 99
 - smishing, 96
 - spam, 98
 - spear phishing, 97
 - SpIT (spam over Internet telephony), 96
 - tailgating, 100–101
 - trust, 93–94
 - typosquatting, 103–104
 - urgency, 94
 - URL hijacking, 103
 - vishing, 96–97
- social media, 105–106
 - impacts, 780
- software, asset inventories, 781–782
- software development, 953
 - Agile software development, 968–969
 - answers to review questions, 1108–1110
 - answers to written labs, 1131
 - APIs (application programming
 - interfaces), 979–980
 - assurance, 958
 - change management and, 976–977
 - code repositories, 981–982

- configuration management and, 976–977
 - DevOps approach, 977–978
 - libraries, 955
 - life cycle models, 970–975
 - OOP (object-oriented programming), 956–958
 - programming languages, 954–955
 - SDLC (software development life cycle), 965
 - SLAs (service-level agreements), 982–983
 - software testing, 980–981
 - spiral model, 967
 - system failure mitigation, 958–961
 - third-party software acquisitions, 983–984
 - tool sets, 955–956
 - waterfall model, 966–967
- software libraries, 955
- software licensing, 166, 183
- software testing, 750
- code review, 751–752
 - DAST (dynamic application security testing), 752
 - exception handling, 750
 - fuzz testing, 754–755
 - IAST (interactive application security testing), 753
 - interface testing, 755–756
 - misuse case testing, 756
 - RASP (Runtime Application Self-Protection), 753
 - SAST (static application security testing), 752
 - test coverage analysis, 757
 - website monitoring, 757
- software-based storage, symmetric keys, 262
- something you are, 650, 656–659
- something you have, 650, 654–655
- something you know, 649, 651–652
- somewhere you are, 650
- SONET (Synchronous Optical Network), 629
- SOP (standard operating procedures), 29
- South African privacy law, 178–179, 183–184
- SOX (Sarbanes-Oxley Act), 181
- spam, 98
- spear phishing, 97
- SpIT (spam over Internet telephony), 96
- split knowledge, 774
- cryptography, 238
- SPOF (single point of failure), 883
- spoofing attacks, 31, 717
- email, 98
- spread spectrum, 536
- spyware, 1016
- SQL injection attacks, 1024–1028
- SRTP (Secure Real-Time Transport Protocol), 522, 587
- SSH (Secure Shell), 518
- SSID (service set identifier), 528–529
- SSO (single sign-on)
- AAA protocols, 698
 - cloud based federation, 664–665
 - FIM (federated identity management) systems, 664–666
 - hybrid federation, 665
 - implementing, 694
 - JIT (Just-in-Time) provisioning, 665–666
 - Kerberos, 698–700
 - on-premises federated identity management system, 665
 - RADIUS, 701
 - TACACS+, 701
- SSRF (server-side request forgery), 1037
- standards, 28
- star topology, 566–567
- state machines, 339
- stateful inspection firewalls, 554, 841
- static, 464–466
- static packet-filtering firewall, 553
- static passwords, 651
- statistical attacks, 306
- steganography, 300–302, 853
- STIX (Structured Threat Information eXpression), 361
- storage
- DBMS (database management system), 994–995
 - evidence storage, 460–461
 - media storage facilities, 459–460
 - symmetric keys, 262
- storage devices
- memory security, 373–374
 - nonvolatile, 373
 - primary storage, 373
 - random access, 373
 - secondary storage, 373
 - security, 374

- sequential, 373
- volatile, 373
- STP (shielded twisted-pair) cabling, 562
- strategic plans, 18
- stream ciphers, 246
- STRIDE threat model, 31
- stripe of mirrors, 884
- striping, 884
- striping with parity, 884
- STs (security targets), 346
- Stuxnet, 1015
- subjects, design, 319–320
- subscription licenses, 166
- substitution ciphers, 240–243
- supervisor state, 367
- swapfiles, 372
- switching
 - circuit switching, 624–625
 - packet switching, 625–626
 - virtual circuits, 626
 - VLANs and, 613–617
- symmetric cryptography
 - 3DES (Triple DES), 256–257
 - AES (Advanced Encryption Standard), 259
 - algorithm comparison, 260–261
 - block cipher modes of operation, 254–256
 - Blowfish, 258
 - CAST algorithms, 260
 - DES (Data Encryption Standard), 256
 - IDEA (International Data Encryption Algorithm), 257–258
 - key management, 261–263
 - RC (Rivest Ciphers), 258–259
 - SKIPJACK, 258
- symmetric key algorithms, 248–250
 - answers to review questions, 1070–1072
 - answers to written labs, 1119–1120
- SYN flood attack, 823–824
- synchronous communications, 569
- system logs, 844
- system resilience, 883
 - RAID array, 884–885
- system security policy, 426
- system sprawl, 405
- systems development lifecycle, 962–965

T

- TACACS (Terminal Access Controller Access Control System), 532–533
- TACACS+ (Terminal Access Controller Access Control System Plus), 701
- tactical plan, 18–19
- tailgating, 100–101
- tamper resistance, 36
- tampering, 31
- tangible assets, 781
- TATO (temporary ATO), 16
- TAXII (Trusted Automated eXchange of Intelligence Information), 361
- TBAC (task-based access control), 688
- TCB (trusted computing base), 333–334
- TCP (Transmission Control Protocol), 505
 - TCP reset attack, 824
- TCP/IP model
 - Application (Process) Layer, 501
 - Internet (Internetworking) Layer, 501
 - Link (Network Interface) Layer, 501
 - OSI Model comparison, 501
 - Transport (Host-to-Host) Layer, 501
- TCSEC (Trusted Computer System Evaluation Criteria), 345
- TDMA (Time Division Multiple Access), 537
- Teardrop attack, 826
- technical controls, 81
- technical physical security controls, 449
- technology convergence, 445
- technology crime investigators, 153
- telecommunications room, 451
- telecommuting, 592
- Telnet, 503
- temperature, 464–466
- TEMPEST (Telecommunications Electronics Material Protected from Emanating Spurious Transmissions), 375
- temporary internet files, 381
- termination policy, 112
- terminations, 56–57, 112
- testing
 - answers to written labs, 1127–1128
 - DRP
 - communications, 911
 - full-interruption test, 909
 - lessons learned test, 909–910

- maintenance, 910
 - parallel test, 909
 - read-through, 908
 - simulation test, 908
 - tabletop, 908
 - walk-through, 908
- fuzz testing, 30
- penetration testing, 3
- software testing, 980–981
- TFTP (Trivial File Transfer Protocol), 503
- third-party connectivity, 622–624
- third-party governance, 15–16
 - processes, 20
 - third-party audit, 21
- third-party liability, cybersecurity
 - insurance and, 76
- third-party security services, 842
- third-party software acquisition, 983–984
- threat actors, 61
- threat agents, 61
- threat events, 62
- threat feeds, 858
- threat hunting, 30, 858–859
- threat intelligence
 - kill chain, 856–857
 - MITRE ATT&CK, 857–858
 - threat feeds, 858
 - threat hunting, 858–859
- threat modeling, 29
 - defensive approach, 30
 - diagramming, 32–33
 - DREAD system, 34–35
 - identifying threats, 30–31
 - individual threats, 32
 - prioritization and response, 33–35
 - proactive approach, 30
 - reduction analysis, 33
- threat vectors, 62
- threats, 61
 - answers to review questions, 1077–1082
 - answers to written labs, 1121–1122
 - identifying, 65–66
- timeliness, 7
- timing attacks, 306
- TKIP (Temporal Key Integrity Protocol), 531
- TLS (Transport Layer Security), 299–300, 518
 - decryptors, 834–835
- TOC (time of check), 1022
- TOCTOU (time of check to time of use), 1022–1023
- tokenization, 211–212, 221, 1041
- top secret data, 192
- top-down approach, 17
- topologies
 - bus topology, 566
 - logical topology, 565
 - mesh topology, 567
 - physical topology, 565
 - ring topology, 565–566
 - star topology, 566–567
- Tor, 300
- total risk, 75
- TOTPs (time-based one-time passwords), 655
- TOU (time of use), 1022
- TPM (Trusted Platform Module), 294, 349–350
- trade secrets, 164–165, 183
- trademarks, 162–163, 183
- traffic analysis, 852
- training
 - exercises, 758–759
 - improving, 108
- training and awareness programs, 761
- transitive trust, 320
- transport architecture, 564–565
- Transport Layer (OSI Model), 496, 498
 - protocols, 504–506
- transposition ciphers, 239–240
- traveling personnel
 - free Wi-Fi, 779
 - malware and monitoring devices, 779
 - sensitive data, 779
 - VPNs (virtual private networks), 779
- trend analysis, 852
- Trojan horses, 1012–1013
- trust
 - social engineering, 93–94
 - transitive trust, 320
- trust anchors, 426
- trusted recovery, 887–888
- truthfulness, 6
- turnstiles, 475
- twisted-pair cabling, 562–563

STP (shielded twisted-pair) cabling, 562
 UTP (unshielded twisted-pair) cabling, 562
 typosquatting, 103–104

U

U.S. privacy law, 168–174, 183–184
 UBA (user behavior analytics), 55, 112
 UDP (User Datagram Protocol), 505–506
 UEBA (user and entity behavior analytics), 55, 112
 UEFI (Unified Extensible Firmware Interface), 378
 UIs (user interfaces), testing, 756
 unclassified data, 192
 unicast technology, 569
 UPS (uninterruptible power supply), 462–463
 urgency, social engineering, 94
 URL filtering, 556
 URL hijacking, 103
 USA PATRIOT Act of 2001, 172
 usability, 7
 USML (United States Munitions List), 167
 UTM (unified threat management), 841
 UTP (unshielded twisted-pair) cabling, 562

V

validity, 6
 Van Eck radiation, 375
 VAST (Visual, Agile, and Simple Threat) threat modeling, 31
 VDC (virtual data center), 403
 VDE (virtual desktop environment), 403
 VDI (virtual desktop infrastructure), 403
 vendor agreements, 58–59
 VENOM (Virtualized Environment Neglected Operations Manipulation), 405
 versioning, change management and, 796
 VIP (virtual IP addresses), 599
 virtual memory, 372
 virtual software, 401–402
 virtualization, 349

containerization and, 406
 OS-virtualization, 406
 security management, 404–405
 virtualized networking, 402
 VM escaping, 405
 virtualized systems, 399–401
 SDx (software-defined everything), 402–404
 virtual software, 401–402
 virtualization security management, 404–405
 virtualized networking, 402
 viruses, 1007–1008
 companion viruses, 1009
 encrypted, 1011
 file infector viruses, 1009
 hoaxes, 1011
 macro viruses, 1009
 MBR (master boot record) and, 1008
 multipartite, 1010
 polymorphic, 1011
 service injection, 1010
 stealth, 1010
 vishing, 96–97, 589–590
 visitor logs, 478
 VLANs (virtual local area networks)
 broadcast storm, 614
 switching and, 613
 distributed virtual switches, 614
 eavesdropping, 615
 MAC cloning, 617
 MAC flooding attack, 616
 VLSM (variable length subnet masking), 515
 VM escaping, 405
 VMI (virtual mobile infrastructure), 403
 VMS (vendor management system), 59–60
 VMs (virtual machines), 398
 voice communications
 phreaking, 589–590
 PSTN (public switched telephone network), 587
 vishing, 589–590
 VoIP, 587–589
 VoIP (voice over IP), 521–522, 587–589
 social engineering, 96
 VPNs (virtual private networks), 606, 607–610, 779
 always-on VPN, 610

- concentrators, 606
 - IPSec, 612–613
 - OpenVPN, 612
 - protocols
 - L2TP, 611
 - PPTP, 611
 - SSH, 612
 - tunneling, 606–607
 - full tunnel, 610
 - split tunnel, 610
 - VSAN (virtual SAN), 403, 523
 - vulnerabilities, 62
 - answers to review questions, 1077–1082
 - answers to written labs, 1121–1122
 - authorization vulnerabilities, 1030–1033
 - CCE (Common Configuration Enumeration), 736
 - client-based systems, 378–381
 - containerization, 406
 - CPE (Common Platform Enumeration), 736
 - CVE (Common Vulnerabilities and Exposures), 736
 - CVSS (Common Vulnerability Scoring System), 736
 - cyber-physical systems, 393
 - DCE (distributed computing environment), 386–387
 - distributed systems, 386–387
 - edge computing, 390–391
 - embedded systems, security concerns, 393–395
 - fog computing, 390–391
 - HPC (high-performance computing), 387–388
 - IaC (infrastructure as code), 397–398
 - ICS (industrial control systems), 384–386
 - identifying, 65–66
 - immutable architecture, 398
 - injection vulnerabilities, 1024–1029
 - IoT (Internet of Things), 389–390
 - microservices, 396–397
 - mobile devices, 407–408
 - deployment policies, 419–424
 - security features, 408–419
 - OVAL (Open Vulnerability and Assessment Language), 736
 - RTOS (real-time OS), 388–389
 - SCAP (Security Content Automation Protocol), 736
 - server-based systems, 381–384
 - static systems, 392–395
 - virtualized systems, 399–405
 - web application vulnerabilities
 - request forgery, 1036–1037
 - session hijacking, 1037
 - XSS (cross-site scripting) attacks, 1033–1036
 - XCCDF (Extensible Configuration Checklist Description Format), 736
 - vulnerability assessment, 3, 735–736
 - compliance checks, 750
 - penetration testing, 747–749
 - vulnerability scans, 736–747
 - vulnerability management
 - CVE (Common Vulnerabilities and Exposures) dictionary, 800–801
 - systems to change, 797
 - unpatched systems, 799
 - vulnerability scanners, 800
 - workflow, 746–747
 - vulnerability scans, 736, 800
 - database vulnerability scans, 745–746
 - network discovery, 737–741
 - network vulnerability scans, 741–743
 - vulnerability management workflow, 746–747
 - web vulnerability scans, 743–745
 - VXLAN (Virtual Extensible LAN), 526
-
- ## W
- WAF (web application firewall), 380, 553, 841
 - WAFs (web application firewalls), 1040
 - WAN technologies, 626–627
 - BPL (broadband over power lines), 628
 - dedicated lines, 627
 - DSL (digital subscriber line), 628
 - fault tolerance, 627
 - ISDN (Integrated Services Digital Network), 628
 - leased lines, 627
 - nondedicated lines, 627

- point-to-point link, 627
- VSAT (very-small-aperture terminal), 628
- warning banners, 837–838
- watermarking, 300–302
 - digital watermarking, 853
- wearable technology, 389
- web application vulnerabilities
 - request forgery, 1036–1037
 - session hijacking, 1037
 - XSS (cross-site scripting) attacks, 1033–1036
- web filtering, 556
- web security gateway, 556
- web vulnerability scans, 743–745
- website monitoring, 757
- well-known ports, 504
- WFPS (Wi-Fi positioning system), 413
- white noise, 375
- whitelisting, 840
- wireless antennas, 534–535
- wireless cells, 530
- wireless communications, 536–537
 - Bluetooth, 537–538
 - NFC (near-field communication), 539
 - RFID (Radio Frequency Identification), 538–539
- wireless networks
 - 802.11 amendments, 527
 - 802.1X/EAP, 532–533
 - ad hoc mode, 528
 - antennas, 534–535
 - attacks, 539–543
 - beacon frame, 529
 - BSSID (basic service set identifier), 529
 - captive portals, 535
 - channels, 529–530
 - ESSID (extended service set identifier), 528
 - fat access point, 528
 - general security procedure, 535–536
 - infrastructure mode, 528
 - SSID (independent service set identifier), 529
 - LEAP (Lightweight Extensible Authentication Protocol), 533

- MAC filter, 534
- OSA (open system authentication), 531
- PEAP (Protected Extensible Authentication Protocol), 533
- security, 530–533
- site surveys, 530
- SKA (shared key authentication), 531
- SSID (service set identifier), 528–529
- thin access point, 528
- WAP (wireless access point), 528
- WEP (Wired Equivalent Privacy), 531
- wireless communications, 536–539
- wireless controller, 528
- WPA (Wi-Fi Protected Access), 531
- WPA2 (Wi-Fi Protected Access 2), 531–532
- WPA3 (Wi-Fi Protected Access 3), 532
- WPS (Wi-Fi Protected Setup), 533
- wiring closets, 450–451
- work area security, 461–462
- work function, cryptography, 238
- workgroup recovery, 891
- workplace privacy, 174
- worms, 1013–1015
- WPS (Wi-Fi Protected Setup), 533

X

- X Window, 503
- XaaS (anything as a service), 789
- XCCDF (Extensible Configuration Checklist Description Format), 736
- XML (eXtensible Markup Language), 694
- XSS (cross-site scripting) attacks, 1033–1036

Z

- zero-day exploits, 826–827, 1018
- zero-knowledge proof, 237–238
- ZTA (zero-trust architecture), 702–703
- ZTNA (zero trust network access), 329
- zzuf tool, 754

