

risk The likelihood of a threat agent taking advantage of a vulnerability and the resulting business impact. A risk is the loss potential, or probability, that a threat will exploit a vulnerability.

risk analysis A detailed examination of the components of risk that is used to ensure that security is cost-effective, relevant, timely, and responsive to threats.

risk assessment A method of identifying vulnerabilities and threats and assessing the possible impacts to determine where to implement security controls.

risk management The process of identifying and assessing risk, reducing it to an acceptable level, and implementing the right mechanisms to maintain that level of risk.

risk-based access control An authorization mechanism that estimates the risk associated with a particular request in real time and, if it doesn't exceed a given threshold, grants the subject access to the requested resource.

role-based access control (RBAC) Type of access control model that provides access to resources based on the role the user holds within the organization or the tasks that the user has been assigned.

rule-based access control (RB-RBAC) Type of access control model that uses specific rules that indicate what can and cannot happen between a subject and an object; built on top of traditional RBAC and is thus commonly called RB-RBAC to disambiguate the otherwise overloaded RBAC acronym.

safeguard A policy, method, technique, or procedure that is put into place to reduce the risk that a threat agent exploits a vulnerability. Also called a countermeasure or control.

sandboxing A type of control that isolates processes from the operating system to prevent security violations.

scoping The process of taking a broader standard and trimming out the irrelevant or otherwise unwanted parts.

secure defaults A secure design principle that entails having every system start off in a state where security trumps user friendliness and functionality, and then has controls deliberately relaxed to enable additional features and generally make the system more user friendly.

Security Assertion Markup Language (SAML) An XML standard that allows the exchange of authentication and authorization data to be shared between security domains.

security awareness The knowledge and attitude of an individual concerning likely threats.

security control Any measure taken by an organization to mitigate information security risks.

security evaluation Assesses the degree of trust and assurance that can be placed in systems for the secure handling of sensitive information.

security information and event management (SIEM) A software platform that aggregates security information and security events and presents them in a single, consistent, and cohesive manner.

security label An identifier that represents the security level of an object.

security orchestration, automation, and response (SOAR) Integrated systems that enable more efficient security operations through automation of various workflows.

security testing Testing all security mechanisms and features within a system to determine the level of protection they provide. Security testing can include penetration testing, formal design and implementation verification, and functional testing.

sensitive information Information that would cause a negative effect on the organization if it were lost or compromised.

sensitivity label A piece of information that represents the security level of an object. Sensitivity labels are used as the basis for mandatory access control (MAC) decisions.

separation of duties A secure design principle that splits up a critical task among two or more individuals to ensure that one person cannot complete a risky task by himself.

serverless architecture A computing architecture in which the services offered to end users, such as compute, storage, or messaging, along with their required configuration and management, can be performed without a requirement from the user to set up any server infrastructure.

service level agreement (SLA) A contract between a service provider and a service user that specifies the minimum acceptable parameters of the services being provided.

shared responsibility A secure design principle that addresses situations in which a service provider is responsible for certain security controls, while the customer is responsible for others.

shoulder surfing When a person looks over another person's shoulder and watches keystrokes or watches data as it appears on the screen in order to uncover information in an unauthorized manner.

simple security property A Bell-LaPadula security model rule that stipulates that a subject cannot read data at a higher security level.

single loss expectancy (SLE) A monetary value that is assigned to a single event that represents the organization's potential loss amount if a specific threat were to take place.

$$\text{asset value} \times \text{exposure factor} = \text{SLE}$$

single sign-on (SSO) A technology that allows a user to authenticate one time and then access resources in the environment without needing to reauthenticate.

social engineering The act of tricking another person into providing confidential information by posing as an individual who is authorized to receive that information.

Software as a Service (SaaS) A cloud computing model that provides users access to a specific application that executes in the service provider's environment.

Software Assurance Maturity Model (SAMM) A maturity model that is specifically focused on secure software development and allows organizations of any size to decide their target maturity levels within each of five critical business functions.

software-defined networking (SDN) An approach to networking that relies on distributed software to provide improved agility and efficiency by centralizing the configuration and control of networking devices.

software-defined security (SDS or SDsec) A security model in which security functions such as firewalling, IDS/IPS, and network segmentation are implemented in software within an SDN environment.

spoofing Presenting false information, usually within packets, to trick other systems and hide the origin of the message. This is usually done by hackers so that their identity cannot be successfully uncovered.

standards Rules indicating how hardware and software should be implemented, used, and maintained. Standards provide a means to ensure that specific technologies, applications, parameters, and procedures are carried out in a uniform way across the organization. They are compulsory.

star property (*-property) A Bell-LaPadula security model rule that stipulates that a subject cannot write data to an object at a lower security level.

static application security testing (SAST) A technique, also called static analysis, that identifies certain software defects or security policy violations by examining the source code without executing the program.

subject An active entity, generally in the form of a person, process, or device, that causes information to flow among objects or that changes the system state.

supervisory control and data acquisition (SCADA) A system for remotely monitoring and controlling physical systems such as power and manufacturing plants.

supply chain An interconnected network of interdependent suppliers and consumers involved in delivering some product or service.

symmetric key cryptography A cryptographic method that uses instances of the same key (called the secret key) for encryption and decryption.

synthetic transaction A transaction that is executed in real time by a software agent to test or monitor the performance of a distributed system.

tabletop exercise (TTX) A type of exercise in which participants respond to notional events to test out procedures and ensure they actually do what they're intended to and that everyone knows their role in responding to the events.

TACACS (Terminal Access Controller Access Control System) A client/server authentication protocol that provides the same type of functionality as RADIUS and is used as a central access control mechanism mainly for remote users.

tailoring The practice of making changes to specific provisions of a standard so they better address organizational requirements.

technical controls Controls that work in software to provide availability, integrity, or confidentiality protection; also called logical access control mechanisms. Some examples are passwords, identification and authentication methods, security devices, auditing, and the configuration of the network.

test coverage A measure of how much of a system is examined by a specific test (or group of tests), which is typically expressed as a percentage.

threat A potential cause of an unwanted incident, which can result in harm to a system or organization.

threat intelligence Evidence-based knowledge about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding responses to that menace or hazard.

threat modeling The process of describing probable adverse effects on an organization's assets caused by specific threat sources.

top-down approach An approach in which the initiation, support, and direction for a project come from top management and work their way down through middle management and then to staff members.

topology The physical construction of how nodes are connected to form a network.

total risk The risk an organization faces if it chooses not to implement any type of safeguard.

trade secret Something that is proprietary to a company and important for its survival and profitability.

trademark A legal right that protects a word, name, product shape, symbol, color, or a combination of these used to identify a product or an organization.

transborder data flow (TDF) The movement of machine-readable data across a political boundary such as a country's border.

Trojan horse A computer program that has an apparently or actually useful function, but that also contains hidden malicious capabilities to exploit a vulnerability and/or provide unauthorized access into a system.

trust but verify A secure design principle that requires that even when an entity and its behaviors are trusted, they should be monitored and verified.

user A person or process that is accessing a computer system.

user and entity behavior analytics (UEBA) Processes that determine normal patterns of behavior so that abnormalities can be detected and investigated.

user ID A unique set of characters or code that is used to identify a specific user to a system.

validation The act of performing tests and evaluations to test a system's security level to see if it complies with security specifications and requirements.

Virtual eXtensible Local Area Network (VxLAN) A network virtualization technology that encapsulates layer 2 frames onto UDP (layer 4) datagrams for distribution anywhere in the world.

virtualization The practice of running a virtual computing system in an environment that is abstracted from the actual hardware.

virus A small application, or string of code, that infects applications. The main function of a virus is to reproduce, and it requires a host application to do this. It can damage data directly or degrade system performance.

vulnerability A weakness in a system that allows a threat source to compromise its security. It can be a software, hardware, procedural, or human weakness that can be exploited.

Waterfall methodology A software development methodology that uses a strictly linear, sequential life-cycle approach in which each phase must be completed in its entirety before the next phase can begin.

whitelist (or allow list) A set of known-good resources such as IP addresses, domain names, or applications.

work factor The estimated time and effort required for an attacker to overcome a security control.

worm An independent program that can reproduce by copying itself from one system to another. It may damage data directly or degrade system performance by tying up resources.

zero trust A secure design principle that assumes that every entity is hostile until proven otherwise.

This page intentionally left blank

INDEX

A

AARs (after-action reviews) in disaster recovery, 869, 1061

ABAC (attribute-based access control)
characteristics, 776
description, 774

ABR (available bit rate) in ATM, 551

abstract machines, 766

abstraction

- containers, 298
- network architectures, 597, 634
- object-oriented programming, 1129
- programming languages, 1119–1120
- system architectures, 283, 297

academic software, 153

acceptable use policies (AUPs)

- software, 226
- user accounts, 858
- web proxies, 664

acceptance risk strategy

- ISO/IEC 27005, 178
- overview, 79–80

acceptance testing in software development, 1091

access control

- authorization mechanisms.
See authentication; authorization
- CPTED, 430–431
- facilities, 443–446, 916–924
- identity and access, 796
- information, 801
- just-in-time, 738
- locks, 917–923
- logical, 717
- markup languages, 776–781
- models, 766
- physical and logical access,
801–803
- physical security. *See* physical security and controls
- remote, 789–795

access control lists (ACLs)

- DAC, 767
- data historians, 293
- identity management, 747
- incident response, 996
- network sockets, 703
- packet-filtering firewalls, 946–948
- RBAC, 771
- routers, 660
- server-based systems, 284
- switches, 657
- VPNs, 697
- WPANs, 571

access doors for data processing facilities, 443

access points (APs)

- collision domains, 493
- DSL modems, 683
- WLANs, 564–565

access triples in Clark-Wilson model, 400

accountability

- audits, 741–745
- credential management, 736
- description, 161, 716
- logical access controls, 717
- overview, 887–888

Accountability Principle in OECD, 142

accounting in Diameter, 795

accounts

- adding, 858
- modifying, 859
- registration and proofing of identity,
738–740
- suspending, 860

accuracy

- biometric systems, 724–725, 727
- data loss prevention, 270
- threat intelligence, 941

ACID properties of database systems, 286

ACK (acknowledgment packets) in TCP

- handshakes, 508, 949–951

ACLs. *See* access control lists (ACLs)

acoustical detection IDSs, 927

- acquired software security concerns, 1145–1148
- acquiring
 - data, 230
 - evidence, 1012–1013
- acrylic windows, 441
- Act phase in Plan-Do-Check-Act loop, 875
- actionability in security metrics, 854
- actions in ABAC, 774
- actions on objectives stage in Cyber Kill Chain framework, 994
- active attacks on cryptography, 367
- Active Directory (AD) environment, 747
- active monitors
 - computer surveillance, 1020
 - Token Ring, 496
- actors
 - defined, 8
 - internal, 61–62
- ad hoc WLANs, 565
- adapters in forensics field kits, 1015
- Address Resolution Protocol (ARP), 515–517
- Adleman, Leonard, 340
- ADM (Architecture Development Method), 194–195
- administrative controls
 - digital asset management, 261
 - risk responses, 83, 86–87
- administrative investigations, 161–162
- administrative law system, 128
- administrative/regulatory law, 130
- administrative responsibilities for locks, 922
- admissibility of evidence, 1013–1014
- ADSL (asymmetric DSL), 684
- Advanced Encryption Standard (AES)
 - DES replacement, 321
 - meeting applications, 694
 - SEDs, 407
 - TLS, 603–604
 - WPA2, 578
 - WPANs, 571
- Advanced Micro Devices (AMD)
 - trade secrets, 149
- Advanced Mobile Phone System (AMPS), 584
- advanced persistent threats (APTs), 135–136
- Advanced Research Project Agency Network (ARPANET) program, 471
- advisory policies, 30
- AE (authenticated encryption), 604
- AEAD (authenticated encryption with additional data), 604
- AES. *See* Advanced Encryption Standard (AES)
- after-action reviews (AARs) in disaster recovery, 869, 1061
- agent based patch management, 904
- agentless patch management, 904
- agents
 - data loss prevention, 273
 - SNMP, 522–523
- aggregation in database systems, 286–287
- Agile methodologies
 - Extreme Programming, 1102
 - Kanban, 1102–1103
 - overview, 1100–1101
 - Scrum, 1101–1102
- agreements
 - disasters recovery, 1047–1048
 - employment, 36–37
 - service level. *See* service level agreements (SLAs)
- AH (Authentication Header) in IPSec, 608
- AIKs (attestation identity keys) in Trusted Platform Modules, 406
- alarms
 - CPTED, 428
 - doors, 444
 - duress codes, 931
 - human-machine interface, 292
 - perimeter security, 803
- ALE (annualized loss expectancy)
 - control selection, 82
 - power backup, 448
 - quantitative risk analysis, 73–75
- algorithms
 - cryptography attacks on, 367–370
 - cryptology, 320–321
 - hashing functions, 351–352
 - patents for, 151
 - public vs. secret, 369
- Align, Plan and Organize (APO) domain in COBIT 2019, 189
- alignment
 - COBIT goals, 188
 - security to business strategy, 13–16, 182, 202
 - strategic, 15–16

- allow lists in IDS/IPS, 968–969
- alternate category in PACE plans, 1057
- always invoked property in reference monitors, 766
- always-on VPN, 697
- AMD (Advanced Micro Devices)
 - trade secrets, 149
- amplification DNS attacks, 620
- amplitude
 - analog signals, 644–645
 - multiplexing systems, 544
 - radio signals, 559–560
- AMPS (Advanced Mobile Phone System), 584
- analog transmission, 644–645
- analysis
 - antimalware software, 970
 - application security, 1139
 - forensics investigations, 1016–1018
 - qualitative risk, 72, 76–78
 - quantitative risk, 72–76, 78–79
 - software security, 1144–1145
- Analysis practice in Good Practice Guidelines, 106
- Android Data company, 150
- annualized loss expectancy (ALE)
 - control selection, 82
 - power backup, 448
 - quantitative risk analysis, 73–75
- annualized rate of occurrence (ARO), 74–75
- annunciator systems in CCTV systems, 916
- anomalies, session termination from, 741
- anomaly-based IDS/IPS, 967–968
- antimalware software, 969–972
- anycast addresses in IPv6, 513
- APIs. *See* application programming interfaces (APIs)
- APO (Align, Plan and Organize) domain
 - in COBIT 2019, 189
- apparent power, 671
- appendices in reports, 873
- Apple lawsuit, 151
- appliances, 958
- application errors in risk management, 54
- application layer
 - functions and protocols, 483
 - OSI model, 474–475
- application-level events in audits, 743
- application-level proxies, 953–955, 957
- application programming interfaces (APIs)
 - application layer, 475
 - CASBs, 275–276
 - containers, 298
 - description, 837
 - object-oriented programming, 1126–1128
 - SDNs, 635
 - software libraries, 1132–1133
 - software security, 1132
 - TEE, 409
 - web services, 613
- applications
 - access control, 802
 - connections, 479
 - security testing, 1139–1140
 - whitelisting, 225
- approval by management, 877
- APs (access points)
 - collision domains, 493
 - DSL modems, 683
 - WLANs, 564–565
- APT32, 389
- APTs (advanced persistent threats), 135–136
- architects for software development, 1080
- Architecture Development Method (ADM), 194–195
- architectures. *See* system architectures
- archive bits for backups, 1035
- archives for data, 239–240
- Arnold, Benedict, 319
- ARO (annualized rate of occurrence), 74–75
- ARP (Address Resolution Protocol), 515–517
- ARPANET (Advanced Research Project Agency Network) program, 471
- artifacts in digital forensics, 1020–1021
- ASOR (authoritative system of record), 739
- ASs (autonomous systems), 533
- assemblers, 1118, 1120–1122
- assembly language, 1118, 1120
- assessments
 - audits, 838–844
 - chapter questions, 846–849
 - chapter review, 844–846
 - designing, 814–815
 - disaster recovery plans, 1058
 - overview, 813
 - physical security, 908
 - preventive and detective measures, 945

- assessments (*cont.*)
 - risk. *See* risk assessment
 - Risk Management Framework, 176
 - social engineering, 903
 - software security, 1144–1148
 - strategies, 813–816
 - technical controls. *See* testing
 - validating, 815–816
- assets
 - business impact analysis, 112–115
 - chapter questions, 247–251
 - chapter review, 245–246
 - classification, 219
 - data life cycle. *See* data life cycle
 - digital, 258–259, 261–263
 - information, 214–219
 - inventories, 224–227
 - life cycle, 222–230
 - overview, 213–214
 - ownership, 223
 - physical security, 220–222
 - provisioning, 227–228
 - retention, 228–230
 - valuation, 65–66
- assisted password resets, 738
- associations in misuse case testing, 835
- ASTM International fire resistance ratings, 456
- asymmetric DSL (ADSL), 684
- asymmetric key cryptography, 328
 - Diffie-Hellman algorithm, 337–340
 - overview, 335–337
 - RSA, 340–342
 - summary, 337
 - with symmetric, 346–349
- asynchronous replication, 1039
- asynchronous token devices for one-time passwords, 731
- Asynchronous Transfer Mode (ATM) in WANs, 550–552
- asynchronous transmissions, 645–647
- atbash cryptology, 317–318
- ATM (Asynchronous Transfer Mode) in WANs, 550–552
- atomic execution in trusted execution environments, 410
- atomicity in ACID properties, 286
- attack surface analysis in software development design, 1085
- attack trees in threat modeling, 386–387
- attacks, evolution of, 134–138
- attenuation in cabling, 652
- attestation identity keys (AIKs) in Trusted Platform Modules, 406
- attocells in Li-Fi standard, 568
- attribute-based access control (ABAC)
 - characteristics, 776
 - description, 774
- attribute-value pairs (AVPs) in RADIUS, 792
- attributes
 - LDAP, 749
 - object-oriented programming, 1125
- audience for reports, 872
- audit-reduction tools, 744
- auditors, 25
- audits
 - accountability, 741–742
 - application-level events, 743
 - external, 842–843
 - internal, 840–842
 - overview, 838–840
 - physical security, 929
 - protecting, 744–745
 - reviewing, 743–744
 - software security, 1147
 - strategies, 813–816
 - system-level events, 742
 - third-party, 843–844
 - user-level events, 743
- AUPs (acceptable use policies)
 - software, 226
 - user accounts, 858
 - web proxies, 664
- authenticated encryption (AE), 604
- authenticated encryption with additional data (AEAD), 604
- authentication. *See also* authorization
 - access control and markup languages, 776–781
 - asymmetric key cryptography, 336
 - biometric. *See* biometric authentication
 - cryptosystems, 323
 - description, 716
 - Diameter, 794–795
 - 802.11, 580

- factors, 718–719
 - Internet of Things, 306
 - Kerberos, 785–788
 - knowledge-based, 720–723
 - network sockets, 703
 - ownership-based, 729–734
 - quorum, 34
 - race conditions, 717
 - VPNs, 697–699
 - Authentication Header (AH) in IPSec, 608
 - authenticators in Kerberos, 786–787
 - authenticity, 6
 - authoritative name servers in DNS, 525
 - authoritative system of record (ASOR), 739
 - authority
 - disaster recovery goals, 1054
 - URLs, 613
 - authorization. *See also* authentication
 - ABAC, 774
 - access control and markup languages, 776–781
 - cryptosystems, 324
 - DAC, 766–768
 - data loss prevention, 267, 271
 - description, 716
 - Diameter, 795
 - e-mail, 624
 - IP telephony, 692
 - Kerberos, 784–789
 - MAC, 768–771
 - OAuth, 782–783
 - OpenID Connect, 783–784
 - overview, 765–766
 - race conditions, 717
 - RB-RBAC, 774
 - risk-based access control, 775–776
 - Risk Management Framework, 176
 - role-based access control, 771–773
 - authorization code flow in OIDC, 784
 - authorization creep
 - description, 395
 - privileged accounts, 889
 - role changes, 799
 - user accounts, 859
 - authorization servers in OAuth, 782
 - auto iris lenses in CCTV systems, 915
 - automated risk analysis methods, 73
 - automated scanning of devices, 226
 - automated tests in software
 - development, 1091
 - automatic tunneling in IPv6, 514
 - automation
 - backups, 863
 - configuration management, 895
 - HMIs, 292
 - SOAR, 980
 - virtualization, 861
 - ZigBee, 571
 - autonomous systems (ASs), 533
 - availability
 - business continuity, 103
 - business continuity planning, 1067–1070
 - CIA triad, 7–8
 - disaster recovery, 1049–1053
 - fault tolerance and system resilience, 1051
 - high, 1050–1053
 - overview, 6
 - quality of service, 1050–1051
 - available bit rate (ABR) in ATM, 551
 - avalanche effect in symmetric key cryptography, 332
 - avoidance risk strategy
 - ISO/IEC 27005, 178
 - overview, 79
 - AVPs (attribute-value pairs) in RADIUS, 792
 - awareness programs
 - content reviews, 43
 - culture factors, 867
 - data protection, 867
 - disaster recovery plans, 1060–1061
 - effectiveness evaluation, 43–44
 - employees, 266
 - goals, 40
 - methods and techniques, 40–44
 - online safety, 866–867
 - overview, 863–864
 - personnel, 930–931
 - social engineering, 864–866
 - AXELOS, 196
- ## B
- B channels in ISDN, 686
 - B2B (business-to-business) transactions in SAML, 780
 - B2C (business-to-consumer) transactions in SAML, 780

- back doors in software development, 1091
- back-off algorithm in CSMA, 491
- background checks in candidate screening and hiring, 35–36
- background elements in reports, 873
- backup administrators, 1035
- backup lighting, 912
- backups
 - vs. archives, 239–240
 - business continuity planning, 1069–1070
 - data loss prevention, 269
 - digital asset management, 261–262
 - electric power, 448–450, 671
 - facilities, 1040–1041
 - hierarchical storage management, 898–899
 - overview, 1034–1037
 - protecting, 896–899
 - restoring, 1037, 1041–1042
 - strategies, 1037–1040
 - verification, 860–862
- BAI (Build, Acquire and Implement) domain in COBIT 2019, 189
- balanced security, 7–8
- bandwidth
 - ATM, 550
 - cable modems, 686–687
 - cabling, 654–655
 - coaxial cable, 649
 - dedicated links, 541–542
 - distribution facilities, 446
 - DSL, 683–684
 - frame relay, 547–548
 - ISDN, 685–686
 - optical carriers, 543
 - proxy servers, 664
 - PVCs, 549
 - QoS, 551–552, 1050
 - satellite communications, 588
 - server-based systems, 300
 - switches, 658
 - unmanaged patching threat, 904
 - VoIP, 688
 - WANs, 543
- barriers in physical security, 908
- BAS (breach and attack simulations), 828
- baseband transmission, 647–648
- Baseline Privacy Interface/Security (BPI/SEC) specifications, 687
- baselines, 31–32
 - anomaly-based IDS/IPS, 968
 - configuration management, 894
 - ISO/IEC 27004, 852
- Basic CIS controls, 187
- Basic Rate Interface (BRI) ISDN, 685–686
- bastion hosts, 965
- BC. *See* business continuity (BC)
- BCM (business continuity management), 102–105
 - enterprise security program, 106–108
 - Professional Practices for Business Continuity Management, 106
- BCP. *See* business continuity planning (BCP)
- beaconing in Token Ring, 496
- beamforming, 567
- behavior blocking in antimalware software, 970–971
- behavioral biometric authentication, 724
- behavioral model for software development design, 1084
- Bell, Alexander Graham, 681
- Bell-LaPadula model, 398–399, 403
- benches, 431
- Berners-Lee, Tim, 253
- best-effort protocols, 503
- best-effort service in QoS, 551
- best practices in business continuity, 104–106
- BGP (Border Gateway Protocol), 536–537
- BIA. *See* business impact analysis (BIA)
- Biba model, 399–400, 403
- big data, retaining, 235
- biometric authentication, 727
 - facial scans, 728
 - fingerprints, 726
 - hand geometry, 727
 - hand topography, 728–729
 - iris scans, 727
 - issues and concerns, 729
 - keystroke dynamics, 728
 - overview, 723–726
 - retina scans, 727
 - signature dynamics, 727–728
 - voice prints, 728
- birthday attacks, 353–354
- BISDN (Broadband ISDN), 685
- bitcoin, 307
- BitTorrent protocol, 149, 307

- black box testing, 826
- black holes, 535, 975
- blacklisting in IDS/IPS, 968–969
- blackouts, 451
- blind penetration testing, 825–826
- block ciphers, 330–333
- Bluejacking, 573
- blueprints in frameworks, 201–203
- Bluesnarfing, 573
- Bluetooth wireless technology, 572–573
- board members, risk reporting for, 94–95
- bollards, 429, 910–911
- BOOTP (Bootstrap Protocol), 519
- Border Gateway Protocol (BGP), 536–537
- botnets, 134
- bots, 134
- boundary conditions in interface testing, 837
- BPC (business process compromise attacks, 59–60
- BPI/SEC (Baseline Privacy Interface/Security) specifications, 687
- branches in tabletop exercises, 1063
- brand issues in disaster recovery, 1054
- BrandScope attacks, 257
- Brazil, General Personal Data Protection Law in, 144
- breach and attack simulations (BAS), 828
- breaches. *See* data breaches
- Brewer and Nash model, 402–403
- BRI (Basic Rate Interface) ISDN, 685–686
- bridges
 - characteristics, 665
 - forwarding tables, 656–657
 - overview, 656
 - vs. routers, 657
- bring your own devices (BYOD), 220
- Broadband ISDN (BISDN), 685
- broadband transmission vs. baseband, 647–648
- broadband wireless access, 569
- broadcast domains in medium access control, 492–494
- broadcast storms in bridges, 656
- broadcast transmission in local area networks, 499–500
- Broken Windows*, 433
- brownouts, 451
- brute-force attacks
 - cryptography, 325, 368
 - passwords, 721
- BSA (Business Software Alliance), 154, 226
- Budapest Convention, 139
- buffer overflows
 - description, 819
 - software development, 1089–1090
- buffers, emulation, 970
- Build, Acquire and Implement (BAI) domain in COBIT 2019, 189
- building codes, 436–437
- bulletproof doors, 440
- bump keys, 924
- bus encryption, 407–408
- bus topology, 487–488
- business continuity (BC)
 - BCP life cycle, 1065–1067
 - business impact analysis, 108–115
 - description, 1030
 - enterprise security program, 106–108
 - overview, 101–104, 867–869, 1065
 - standards and best practices, 104–106
- Business Continuity Institute, Good Practice Guidelines, 105–106
- business continuity management (BCM), 102–105
 - enterprise security program, 106–108
 - Professional Practices for Business Continuity Management, 106
- business continuity planning (BCP), 101–105
 - end-user environment, 1071
 - enterprise security program, 108
 - hardware backups, 1069–1070
 - information systems availability, 1067–1070
 - life cycle, 1065–1067
 - overview, 107, 1065
 - storing, 1042
 - teams, 1030
- business critical data in disaster recovery, 1032
- business enablement, 16
- business entry rule in evidence admissibility, 1014

- business impact analysis (BIA), 104–105
 - asset value, 112–115
 - disaster recovery, 1032
 - overview, 108–109
 - risk assessment, 109–112
 - steps, 112
- business process compromise (BPC) attacks, 59–60
- business process recovery, 1033–1034
- Business Software Alliance (BSA), 154, 226
- business strategy, aligning security to, 13–16
- business-to-business (B2B) transactions
 - in SAML, 780
- business-to-consumer (B2C) transactions
 - in SAML, 780
- business unit leads on incident response teams, 1001
- business units in incident notifications, 1004
- BYE messages in SIP, 689–690
- BYOD (bring your own devices), 220
- bytecode in Java programming language, 1122–1123

C

- C programming language, 1121–1122
- cable modems, 686–687
- cable traps, 921
- cabling
 - bandwidth and throughput, 654–655
 - coaxial cable, 649
 - fiber-optic cable, 650–651
 - forensics field kits, 1015
 - overview, 648
 - problems, 651–653
 - twisted-pair cabling, 649–650
- CABs (change advisory boards)
 - policies for, 891
 - purpose, 93
 - software development tools, 1138
- cache poisoning, ARP table, 516–517
- Caesar, Julius, 318
- Caesar cipher, 318–319
- California Consumer Privacy Act (CCPA), 141–142
- call-processing managers, 688
- call trees in disaster recovery plans, 1056
- cameras in CCTV systems, 916
- CAN (Controller Area Network) bus, 627
- Canada, Personal Information Protection and Electronic Documents Act in, 147
- Capability Maturity Model (CMM), 197–199
- Capability Maturity Model Integration (CMMI), 1107–1109
- capacitance detectors, 927
- CAPTCHA data, 723
- card badge readers, 925
- care-of addresses in mobile IP, 793
- carrier sense multiple access (CSMA), 490–491
- carrier sense multiple access with collision avoidance (CSMA/CA), 491
- carrier sense multiple access with collision detection (CSMA/CD), 491
- carriers in steganography, 265
- CART acronym in threat intelligence, 941
- CAs (certificate authorities), 360–362
- CASBs (cloud access security brokers), 275–276
- cascading errors, 62
- CASE (computer-aided software engineering) tools, 1087
- catastrophes, 1043
- categorize step in Risk Management Framework, 174–175
- CBC-MAC (CCM), 578
- CBEST standard, 156
- CBKE (Certificate-Based Key Establishment) protocol, 572
- CBR (constant bit rate) in ATM, 551
- CCDs (charged-coupled devices), 914
- CCM (CBC-MAC), 578
- CCPA (California Consumer Privacy Act), 141–142
- CCTV (closed-circuit TV) systems, 913–916
- CD (continuous delivery) in software security, 1140–1141
- CDDI (Copper Distributed Data Interface), 497
- CDIs (constrained data items) in Clark-Wilson model, 400
- CDMA (code division multiple access), 584–585
- CDNs (content distribution networks), 308, 674

- ceilings
 - considerations, 437
 - dropped, 442
 - RFI issues, 450
- cell suppression in database systems, 288
- Center for Internet Security (CIS) framework
 - CIS Controls Measures and Metrics document, 92
 - security controls, 172, 185–187
- centralized patch management, 904–905
- Centripetal Networks, 151
- CEOs (chief executive officers), 19–21
- CER (crossover error rate) in biometric authentication, 724–725
- CERT (Computer Emergency Response Team), 993
- CERT Advisory for privacy issues, 1014
- CERT/CC (Computer Emergency Response Team Coordination Center), 901
- certificate authorities (CAs), 360–362
- Certificate-Based Key Establishment (CBKE) protocol, 572
- certificate revocation lists (CRLs), 361–362
- certificates in PKI, 359–360
- certifications, 40–41
- CFOs (chief financial officers), 19–20
- chain of custody for evidence, 1010–1011
- Challenge Handshake Authentication Protocol (CHAP), 698
- change
 - data loss prevention for, 270
 - digital asset management, 262
 - monitoring, 92–93
- change advisory boards (CABs)
 - policies for, 891
 - purpose, 93
 - software development tools, 1138
- change control analysts, 24
- change management, 891
 - vs. configuration management, 895
 - documentation, 893
 - practices, 891–892
 - runbooks, 1006
 - software development, 1092–1094
 - software security, 1145
- change management boards, 223
- channel service unit/data service unit (CSU/DSU), 543–545
- channels
 - access points, 565
 - for attacks, 474
- CHAP (Challenge Handshake Authentication Protocol), 698
- charged-coupled devices (CCDs), 914
- Check phase in Plan-Do-Check-Act loop, 875
- checkers, password, 722
- checklist tests in disaster recovery plans, 1062–1063
- chemical fire extinguishers, 459
- chests for data protection, 222
- Cheyenne Mountain complex, 436
- chief executive officers (CEOs), 19–21
- chief financial officers (CFOs), 19–20
- chief human resources officers (CHROs), 990
- chief information officers (CIOs), 19–21, 990
- chief information security officers (CISOs)
 - IMPs, 990
 - incident notifications, 1004
 - incident response teams, 1001
 - role, 22
- chief operations officers (COOs), 990
- chief privacy officers (CPOs), 21
- chief security officers (CSOs), 22
- Chinese Remainder Theorem (RSA-CRT), 372
- Chinese Wall model, 402–403
- chipping code in DSSS, 562
- chips in DSSS, 562
- chosen-ciphertext attacks, 369
- chosen-plaintext attacks, 368–369
- CHROs (chief human resources officers), 990
- CI (continuous integration) in software security, 1140–1141
- CIA triad, 7–8
- CIDR (classless interdomain routing), 512
- CIOs (chief information officers), 19–21, 990
- cipher locks, 920–921
- ciphers in cryptography, 318–321
- ciphertext-only attacks, 368
- CIR (committed information rate) in frame relay, 547–548
- circuit-level proxies, 953–957
- circuit switching in WANs, 545–547
- circumventing locks, 922–924

- CIS (Center for Internet Security) framework
 - CIS Controls Measures and Metrics document, 92
 - security controls, 172, 185–187
- Cisco Systems, 151
- CISOs. *See* chief information security officers (CISOs)
- civil investigations, 162
- civil law, 126–129
- Clark-Wilson model, 400, 403
- classes
 - IP addresses, 510
 - object-oriented programming, 1125–1127
- classification
 - artificial intelligence tools, 977
 - data retention, 236
 - incidents, 1002–1003
 - information, 215–219
- classless interdomain routing (CIDR), 512
- classless IP addresses, 512
- clean desk policy, 442–443
- cleanroom methodology in software development, 1105
- clearing media, 259
- client-based systems, 284
- client/server systems, 284
- clipping levels for failed logon attempts, 721
- close stage in change management, 892
- CLOSE-WAIT state in TCP connections, 951
- closed-circuit TV (CCTV) systems, 913–916
- CLOSING state in TCP connections, 951
- cloud access security brokers (CASBs), 275–276
- cloud-based systems
 - asset provisioning, 228
 - backups, 1038
 - deployment models, 305
 - FIM systems, 756
 - frame relay, 548
 - IaaS, 304
 - overview, 301–302
 - PaaS, 302–304
 - SaaS, 302–303
 - XaaS, 304–305
- clustered servers in quality of service, 1051
- clustering for artificial intelligence tools, 978
- CM. *See* configuration management (CM)
- CMDB (configuration management database), 895
- CMF (collection management framework)
 - forensics investigations, 1016–1017
 - logs, 978
 - threat intelligence, 942
- CMM (Capability Maturity Model), 197–199
- CMMI (Capability Maturity Model Integration), 1107–1109
- CO₂ fire suppression, 458
- coaxial cable, 649
- COBIT 2019 framework, 172, 187–189
- code and coding
 - bloat, 833
 - obfuscation, 905
 - repositories, 1143–1144
 - reviews, 833–834
 - secure practices, 1134–1136
 - testing, 834–835
- code division multiple access (CDMA), 584–585
- code law, 126
- Code of Ethics, 44–45
- Codecov platform, 1141
- CoE (Council of Europe), 139
- cognitive passwords, 723
- cohesion in software, 1130–1132
- COI (community of interest) as threat data source, 943
- cold sites in disaster recovery, 1045–1047
- collection
 - data, 231–232
 - evidence, 1010–1012
- Collection Limitation Principle in OECD, 142
- collection management framework (CMF)
 - forensics investigations, 1016–1017
 - logs, 978
 - threat intelligence, 942
- collision free hashing algorithms, 351–352
- collisions
 - CSMA, 490
 - hashing functions, 353
 - medium access control, 492–494
- collusion, 34
- COM domain in DNS, 527
- combi smart cards, 734
- combination locks, 920
- Command and Control
 - Cyber Kill Chain model, 388, 994
 - MITRE ATT&CK framework, 389

- commercial off-the-shelf (COTS) software
 - description, 153
 - security concerns, 1146
- committed information rate (CIR) in frame relay, 547–548
- common controls in Risk Management Framework, 175
- common law, 126–130
- Common Weakness Enumeration (CWE) initiative, 1088
- communication
 - audit results, 839–840
 - in disaster recovery plans, 1056–1057
 - employees, 266
 - object-oriented programming, 1126
- communications channels
 - chapter questions, 709–712
 - chapter review, 707–709
 - data, 702–704
 - multimedia collaboration, 693–696
 - overview, 681
 - remote access, 696–702
 - third-party connectivity, 705–706
 - virtualized networks, 704–705
 - voice. *See* voice communications
- community clouds, 305
- community of interest (COI) as threat data source, 943
- community strings in SNMP, 522–524
- comparability of security metrics, 854–855
- compartmentalizing information in forensics investigation interviews, 1019
- compensating controls in risk responses, 85, 87–88
- compiled code, software escrow for, 1143
- compilers, 1119–1122
- complete characteristic of threat intelligence, 941
- complexities in cybercrimes, 132–134
- compliance
 - audits, 844
 - chapter questions, 165–169
 - chapter review, 162–165
 - checks, 838
 - cybercrimes, 130–139
 - data breaches, 139–147
 - identity and access, 796–797
 - investigation requirements, 161–162
 - laws and regulations, 125–130
 - liability and ramifications, 158–161
 - licensing and intellectual property requirements, 147–154
 - monitoring, 93–94
 - overview, 125
 - policies, 39–40
 - requirements, 155–161
- compromise assessments, 17
- computer-aided software engineering (CASE) tools, 1087
- computer-assisted crimes, 130–131
- Computer Emergency Response Team (CERT), 993
- Computer Emergency Response Team Coordination Center (CERT/CC), 901
- Computer Ethics Institute, 45–46
- “computer is incidental” crimes, 130–131
- computer surveillance, 1020
- computer system connections, 479
- computer-targeted crimes, 130–131
- concentrators, 655
- concurrency management in software, 1142
- conference call bridges in H.323, 689
- confidential classification level, 216–217
- confidentiality
 - asymmetric key cryptography, 336
 - audit logs, 745
 - Bell-LaPadula model, 398
 - business continuity, 102–103
 - CIA triad, 8, 64
 - cryptosystems, 323–324, 330
 - customer relations, 174–175
 - DNS over HTTPS, 621
 - forensics investigation interviews, 1019
 - overview, 4–5
 - TLS, 602
 - VPNs, 605
- configuration management (CM)
 - automation, 895
 - baselining, 894
 - vs. change management, 895
 - identity and access, 799
 - overview, 893–894
 - preventive and detective measures, 944
 - provisioning, 894–895
 - secure software, 1142
 - unmanaged patching threat, 904

- configuration management database (CMDB), 895
- confusion in symmetric key cryptography, 331
- congestion
 - TCP vs. UDP, 503, 506
 - throughput, 654
- connection-oriented protocols
 - description, 479
 - TCP, 503–504
- connectionless protocols
 - description, 479
 - UDP, 503–504
- connections in TCP vs. UDP, 506
- connectivity for federated identity, 754–755
- consent provision in GDPR, 144–145
- consistency in ACID properties, 286
- constant bit rate (CBR) in ATM, 551
- constrained data items (CDIs) in Clark-Wilson model, 400
- construction issues, 436–439
- consultants, 39
- consumer-grade products for meeting applications, 694
- contact smart cards, 733
- contactless smart cards, 733–734
- containerization, 298–299
- content-dependent access control in database systems, 287
- content distribution networks (CDNs), 308, 674
- content reviews, periodic, 43
- context-dependent access control for database systems, 287–288
- context in ABAC, 774
- contingency category in PACE plans, 1057
- contingency strategies in business continuity, 104–105
- contingency suppliers in disaster recovery, 1046
- continuous delivery (CD) in software security, 1140–1141
- continuous improvement in risk management, 95–96
- continuous integration (CI) in software security, 1140–1141
- continuous lighting, 912
- continuous monitoring, 981–982
- contractors, 39
- contractual requirements compliance, 156–158
- control planes in SDNs, 633–634
- control zones, 803
- controlled unclassified data, 216–217
- Controller Area Network (CAN) bus, 627
- controllers, data, 244
- controls
 - assessments. *See* testing
 - CPTED, 430–431
 - data states, 254–258
 - defined, 9
 - digital asset management, 261–262
 - frameworks, 172, 183–189
 - overview, 253–254
 - preventive and detective measures, 944
 - scoping and tailoring, 258
 - standards, 258
 - threat modeling, 387
- controls for risk response
 - assessments, 88–91
 - selection, 82–83
 - types, 83–88
- controls for secure software
 - application testing, 1139–1140
 - code repositories, 1143–1144
 - continuous integration and delivery, 1140–1141
 - development platforms, 1137–1138
 - overview, 1136–1137
 - SOAR, 1141–1142
 - software configuration management, 1142
 - tool sets, 1138
- controls for site and facilities
 - data processing facilities, 443–446
 - distribution facilities, 446–447
 - environmental issues, 461
 - fire safety, 454–460
 - storage facilities, 447–448
 - utilities, 448–454
 - work area security, 441–443
- Convention on Cybercrime, 139
- converged protocols, 627–628
- cookies for web services, 613
- coordinators in WPANs, 570
- COOs (chief operations officers), 990
- copper cable, 649–650
- Copper Distributed Data Interface (CDDI), 497
- Copyright Directive, 155

- copyrights, 149–150
- core RBAC, 772
- corrective controls in risk response, 85, 87
- cost approach in executive summaries, 874
- cost/benefit comparisons in risk assessment, 64, 82
- costs
 - outsourced security services, 974
 - smart cards, 734
- COTS (commercial off-the-shelf) software
 - description, 153
 - security concerns, 1146
- Council of Europe (CoE), 139
- Counter Mode Cipher Block Chaining Message Authentication Code Protocol, 578
- countermeasures
 - defined, 9
 - risk responses, 81–83
- coupling in software, 1130–1132
- coverage for backups, 863
- covert channels, 401
- covert timing channels, 401
- CPOs (chief privacy officers), 21
- CPTED. *See* Crime Prevention Through Environmental Design (CPTED)
- crackers for passwords, 722
- create, read, update, and delete (CRUD)
 - actions for database systems, 285–287
- credential management
 - accountability, 741–745
 - just-in-time access, 738
 - overview, 736
 - password managers, 736–737
 - password resets, 737–738
 - password synchronization, 737
 - profile updates, 740
 - registration and proofing of identity, 738–740
 - session management, 740–741
 - unmanaged patching threat, 904
- Crime Prevention Through Environmental Design (CPTED)
 - landscaping, 908
 - maintenance, 433
 - natural access control, 428–431
 - natural surveillance, 431
 - overview, 427–428
 - territorial reinforcement, 431–432
- crimes. *See also* incidents
 - crime scene control, 1010
 - detection goals, 424
 - evidence collection and handling, 1008
 - incident investigations, 1006–1008
 - incident response, 992
 - investigation requirements, 162
- criminal law system, 127, 129
- critical data backups, 1037
- criticality of data, 215
- criticality values in disaster recovery, 1032
- CRLs (certificate revocation lists), 361–362
- cross-certification, 361
- cross-sectional photoelectric cells, 927
- crossover error rate (CER) in biometric authentication, 724–725
- crosstalk in cabling, 653
- CRUD (create, read, update, and delete)
 - actions for database systems, 285–287
- cryptanalysis, 317
- cryptographic hash chaining, 831
- cryptology. *See also* encryption
 - asymmetric key, 335–342
 - attacks against, 367–375
 - chapter questions, 379–383
 - chapter review, 375–378
 - cryptosystems, 323–325
 - definitions and concepts, 321–323
 - ECC, 342–343
 - hardware vs. software systems, 602
 - history, 317–321
 - hybrid encryption methods, 346–350
 - integrity, 351–358
 - IP telephony, 692
 - Kerckhoffs' Principle, 324–325
 - life cycle, 328
 - methods overview, 328
 - one-time pads, 325–328
 - overview, 317
 - PKI, 359–367
 - quantum, 344–346
 - symmetric key, 329–335
- cryptoprocessors for bus encryption, 408
- cryptosystems
 - components, 323–324
 - description, 321
 - strength, 325

- cryptovariables, 322
- CSMA (carrier sense multiple access), 490–491
- CSMA/CA (carrier sense multiple access with collision avoidance), 491
- CSMA/CD (carrier sense multiple access with collision detection), 491
- CSOs (chief security officers), 22
- CSU/DSU (channel service unit/data service unit), 543–545
- culture
 - data prevention strategies, 269
 - DevOps, 1104
 - employee matches, 35
 - internal audits, 841
 - risk analysis teams, 76, 78
 - security awareness, 867
- current in electrical power, 670
- custodians, data, 244
- customary law system, 128
- customers
 - confidentiality for, 174–175
 - incident notifications to, 1004
- CWE (Common Weakness Enumeration) initiative, 1088
- Cyber Kill Chain framework, 387–389, 994–995
- cyber-physical systems, 306
- cybercrimes and data breaches
 - common schemes, 137
 - complexities, 132–134
 - evolution of attacks, 134–138
 - international issues, 138–139
 - overview, 130–132
- cybercriminals, 60
- cybersecurity analysts
 - incident response teams, 1001
 - tasks and responsibilities, 886
- Cybersecurity Framework, 172, 182
- cybersecurity governance
 - aligning security to business strategy, 13–16
 - authenticity, 6
 - availability, 6
 - balanced security, 7–8
 - baselines, 31–32
 - chapter questions, 48–52
 - chapter review, 46–48
 - concepts and terms, 4–10

- confidentiality, 5
- education and training, 40–44
- guidelines, 32
- implementation, 32–33
- integrity, 5–6
- miscellaneous terms, 8–10
- nonrepudiation, 6–7
- organizational processes, 17–18
- organizational roles and responsibilities, 18–25
- overview, 3–4
- personnel security, 33–40
- principles, 10–12
- procedures, 32
- professional ethics, 44–46
- security overview, 25–27
- security policies, 27–29
- standards, 29–31
- cyberthreat hunting, 943

D

- D-AMPS (Digital AMPS), 584
- D channels in ISDN, 686
- DAC (discretionary access control)
 - challenges, 768
 - characteristics, 776
 - overview, 766–767
- DACs (dual-attached concentrators)
 - in FDDI, 498
- damage assessment in disaster recovery plans, 1058
- DASs (data acquisition servers)
 - in SCADA systems, 294
- DASs (dual-attachment stations)
 - in FDDI, 498
- DAST (dynamic application security testing), 1139
- data
 - acquisition, 230
 - archival, 239–240
 - backups, 861–862, 1034–1041
 - classification, 215–216
 - collection, 231–232
 - destruction, 240–244
 - roles, 244–245
 - sharing, 238–239
 - storage, 232–233
 - use, 237–238

- data acquisition servers (DASs) in SCADA systems, 294
- data analysts, 24
- data at rest
 - description, 59
 - overview, 254–255
- data breaches
 - Codecov, 1141
 - European Union Laws, 142–144
 - GDPR, 144
 - import/export controls, 145–146
 - overview, 139–141
 - PII, 140–141
 - privacy, 147
 - transborder data flow, 146–147
 - U.S. laws, 141–142
- data communications, 702
 - application layer, 474–475
 - data link layer, 480–483
 - functions and protocols, 483–485
 - layers together, 485–487
 - network layer, 480
 - network reference models, 470–471
 - network sockets, 703
 - overview, 469–470
 - physical layer, 483
 - presentation layer, 475–476
 - protocols, 471–474
 - remote procedure calls, 703–704
 - session layer, 477–478
 - transport layer, 479–480
- data controllers in GDPR, 143
- data custodians, 23
- data diodes, 293, 831
- Data Encryption Standard (DES), 321
- data flows in data loss prevention, 268–269
- data hiding in object-oriented programming, 1128
- data historians, 293
- data in motion/transit
 - description, 59
 - overview, 254–256
- data in use
 - description, 59
 - overview, 254, 256–258
- data leaks, 267
- data life cycle
 - data acquisition, 230
 - data archival, 239–240
 - data collection, 231–232
 - data destruction, 240–244
 - data loss prevention, 269
 - data retention, 233–236
 - data roles, 244–245
 - data sharing, 238–239
 - data storage, 232–233
 - data use, 237–238
 - e-discovery, 236–237
 - overview, 230
- data link layer
 - functions and protocols, 484–485
 - OSI model, 480–483
 - protocols, 646
- data localization laws, 146–147, 232
- data loss prevention (DLP)
 - approaches, 267
 - awareness programs, 867
 - data flows, 268–269
 - endpoint, 273–274
 - hybrid, 274
 - inventories, 267–268
 - network, 272–273
 - overview, 265–267
 - protection strategies, 269–271
 - SOAR, 1142
- Data-Over-Cable Service Interface Specifications (DOCSIS), 687
- data owners, 22–23
- data processing facilities, 443–446
- data processors in GDPR, 143
- Data Protection Directive (DPD), 143
- data protection methods
 - cloud access security brokers, 275–276
 - data loss prevention, 265–274
 - digital asset management, 261–263
 - Digital Rights Management, 263–265
 - overview, 258–261
- Data Protection Officers (DPOs)
 - in GDPR, 144
- Data Quality Principle in OECD, 142
- data retention
 - overview, 233
 - policies, 234–236

- data security
 - chapter questions, 277–279
 - chapter review, 276–277
 - controls, 253–258
 - overview, 253
 - protection methods. *See* data protection methods
 - supply chain risk management, 100
- data sovereignty laws, 232
- data states in controls, 254–258
- data structures in TCP, 509
- data subjects in GDPR, 143
- database management systems (DBMSs), 285–286
- database systems, 285
 - ACID properties, 286
 - backups, 861
 - directory services, 747
 - securing, 286–288
- dating evidence, 1010
- DBMSs (database management systems), 285–286
- DCs (domain controllers) in directory services, 747–748
- DCSs (distributed control systems), 290, 293
- DDoS (distributed denial-of-service) attacks
 - CDNs for, 674
 - DNS, 619–620
 - PaaS for, 303
- DDR (dial-on-demand routing), 686
- decision stage in forensics investigations, 1016–1017
- decommissioning assets, 229–230
- dedicated lines for WANs, 541–543, 552
- defaults
 - network, 598
 - secure, 396–397, 422
 - third-party connectivity, 706
 - web services, 611
- defects per KLOC, 395
- defense in depth
 - controls for, 84
 - design principle, 390–392
 - HTTPS, 614
 - network security, 598
 - physical security, 906
 - site and facility security, 419
 - third-party connectivity, 706
- deferred commitment in object-oriented programming, 1127
- defined level in CMMI, 1108
- degaussing media, 243, 261
- degrees, 40–41
- delay time for locks, 918, 920
- delayed loss risk, 63
- delaying mechanisms in site planning, 424
- Deliver, Service and Support (DSS) domain in COBIT 2019, 189
- delivery stage in Cyber Kill Chain model, 388, 994
- Delphi technique, 77
- deluge water sprinkler systems, 460
- DeMarco, Tom, 283
- demilitarized zones (DMZs) for firewalls
 - dual-homed, 959
 - functions, 945–946
 - screened subnet, 960
- denial-of-service (DoS) attacks
 - STRIDE model, 388
 - wireless communications, 578
- Denis Trojan, 389
- deny lists in IDS/IPS, 968–969
- Department of Defense Architecture Framework (DoDAF), 173, 195
- depositories, protecting, 222
- deprovisioning accounts, 800
- depth of field in CCTV systems, 915
- DES (Data Encryption Standard), 321
- design
 - assessments, 814–815
 - network security, 597–599
 - SDLC, 1080, 1083–1087
 - secure. *See* secure design principles
 - site and facility security, 417–418
 - software. *See* secure software; software development
- Design function in SAMM, 1109
- Design practice in Good Practice Guidelines, 106
- desktop virtualization, 699–701
- destroying data, 240–244
- detection
 - fire safety, 454–457
 - Framework Core, 182
 - incidents, 995–996

- detective controls in risk responses, 85, 87
- deterrent controls in risk responses, 85, 87
- deterrents in physical security, 908
- development platforms for software, 1137–1138
- development stage in SDLC, 1080, 1087–1089
- device locks, 922–923
- devices
 - access control, 802
 - industrial control systems, 291–293
 - IP telephony, 688
 - management software, 226
- DevOps, 1103–1104
- DevSecOps
 - software development, 1104
 - software security, 1144–1145
- DFS (Dynamic Frequency Selection), 574
- DGAs (domain generation algorithms) in DNS, 617–618
- DHCP (Dynamic Host Configuration Protocol)
 - IP addresses, 501
 - overview, 517–519
- DHCPACK packets, 518–519
- DHCPDISCOVER packets, 518–519
- DHCPOFFER packets, 518–519
- DHCPREQUEST packets, 518–519
- diagonal filters in QKD, 344
- diagrams, network, 668–670
- dial-on-demand routing (DDR), 686
- dial-up connections, 684
- dialog management, 477
- Diameter protocol, 793–795
- dictionary attacks on passwords, 721
- differential backups, 1035–1036
- differential cryptanalysis attacks, 369–370
- differential power analysis for smart cards, 735
- differentiated service in QoS, 551
- Diffie, Whitfield, 337–340
- Diffie-Hellman algorithm, 337–340
- diffusion in symmetric key cryptography, 331–332
- digital acquisition of evidence, 1012
- Digital AMPS (D-AMPS), 584
- digital certificates in PKI, 359–360
- digital forensics
 - artifacts, 1020–1021
 - field kits, 1015
 - interviews, 1018–1019
 - investigation techniques, 1016–1018
 - overview, 1015–1016
 - reporting and documenting, 1021–1022
 - surveillance, 1019–1020
 - undercover investigations, 1020
- Digital Millennium Copyright Act (DMCA), 154
- Digital Rights Management (DRM), 263–265
- Digital Signature Algorithm (DSA), 357–358
- Digital Signature Standard (DSS), 352, 357
- digital signatures for message verification, 356–358
- digital subscriber lines (DSLs), 648, 683–685
- digital transmission, 644–645
- digital video recording (DVR) systems, 913
- digital zoom in CCTV systems, 915
- dignitary wrongs category in civil law, 128
- diode lasers in fiber-optic cable, 651
- dips in electric power, 451
- direct-attached storage for backups, 1038
- direct sequence spread spectrum (DSSS), 562–563
- directors of security operations in incident response teams, 1001
- directory permissions, testing, 821
- directory roles in identity management, 748–750
- directory services, 747–748
- disassembly tools in forensics field kits, 1015
- disaster recovery (DR)
 - availability issues, 1049–1053
 - description, 101, 1029–1030
 - incident response, 992
 - overview, 867–869
 - process overview, 1053–1055
- disaster recovery plans (DRPs)
 - assessment, 1058
 - communications, 1056–1057
 - contents, 1055
 - description, 101
 - lessons learned, 1061
 - personnel, 1055–1056
 - responses, 1055
 - restoration, 1058–1060

- ul style="list-style-type: none;">
- disaster recovery plans (DRPs) (*cont.*)
 - storing, 1042
 - testing, 1061–1065
 - training and awareness, 1060–1061
- disasters
 - business continuity, 1065–1071
 - business process recovery, 1033–1034
 - chapter questions, 1073–1076
 - chapter review, 1071–1073
 - data backups, 1034–1041
 - description, 1043
 - documentation, 1041–1042
 - human resources, 1042–1043
 - overview, 1029
 - reciprocal agreements, 1047–1048
 - recovery site strategies, 1043–1047
 - recovery strategies overview, 1029–1033
 - redundant sites, 1048–1049
- disc tumbler locks, 919
- discovery step in penetration testing, 824
- discrepancies in identity, 798–799
- discretionary access control (DAC)
 - challenges, 768
 - characteristics, 776
 - overview, 766–767
- disposal of digital asset management, 262
- disruption prevention in site planning, 424
- distance-vector routing protocols, 535
- distinguished names (DNs)
 - directory services, 747–748
 - LDAP, 749
- distributed control systems (DCSs), 290, 293
- distributed denial-of-service (DDoS) attacks
 - CDNs for, 674
 - DNS, 619–620
 - PaaS for, 303
- Distributed Network Protocol 3 (DNP3), 626–627
- distributed systems, 307–309
- distribution facilities, 446–447
- divestitures, 17–18
- DKIM (DomainKeys Identified Mail), 625
- DLP. *See* data loss prevention (DLP)
- DMARC (Domain-based Message Authentication, Reporting and Conformance) system, 625
- DMCA (Digital Millennium Copyright Act), 154
- DMZs (demilitarized zones) for firewalls
 - dual-homed, 959
 - functions, 945–946
 - screened subnet, 960
- DNP3 (Distributed Network Protocol 3), 626–627
- DNS. *See* Domain Name Service (DNS)
- DNs (distinguished names)
 - directory services, 747–748
 - LDAP, 749
- DNS over HTTPS (DoH), 621
- DNSSEC (DNS security)
 - overview, 620–621
 - threats, 529–531
- Do phase in Plan-Do-Check-Act loop, 875
- DOCSIS (Data-Over-Cable Service Interface Specifications), 687
- documentation
 - audits, 839–840
 - backups, 863
 - change management, 262, 893
 - digital forensics, 1021–1022
 - disaster recovery, 1041–1042
 - forensics field kits, 1015
 - incident response, 992
 - software vulnerability scans, 901
- DoDAF (Department of Defense Architecture Framework), 173, 195
- dogs, 929
- DoH (DNS over HTTPS), 621
- Domain-based Message Authentication, Reporting and Conformance (DMARC) system, 625
- domain controllers (DCs) in directory services, 747–748
- domain generation algorithms (DGAs) in DNS, 617–618
- Domain Name Service (DNS)
 - attack prevention, 617–620
 - DNS over HTTPS, 621
 - DNSSEC, 620–621
 - domains, 526–527
 - filters, 621
 - MITRE ATT&CK framework, 389
 - overview, 524–526, 616
 - resolution components, 527–528
 - splitting, 530
 - threats, 529–531

- DomainKeys Identified Mail (DKIM), 625
 - domains
 - collision and broadcast, 492–494
 - DNS, 526–527
 - doors
 - considerations, 437
 - data processing facilities, 443
 - lock delay feature, 920
 - types, 440–441
 - DoS (denial-of-service) attacks
 - STRIDE model, 388
 - wireless communications, 578
 - double-blind penetration tests, 826
 - double tagging attacks on VLANs, 632
 - downstream liability, 39, 161
 - downstream suppliers in risk management, 98
 - downtime in high availability, 1050
 - DPD (Data Protection Directive), 143
 - DPOs (Data Protection Officers)
 - in GDPR, 144
 - DR. *See* disaster recovery (DR)
 - draft IEEE 802.11i, 576
 - DRI International Institute, Professional Practices for Business Continuity Management, 106
 - drive-by downloads, 865
 - drives, self-encrypting, 407
 - DRM (Digital Rights Management), 263–265
 - dropped ceilings, 442
 - DRPs. *See* disaster recovery plans (DRPs)
 - dry pipe water sprinkler systems, 460
 - DSA (Digital Signature Algorithm), 357–358
 - DSD (dynamic separation of duty)
 - relations, 773
 - DSLAMs (DSL access multiplexers), 683
 - DSLs (digital subscriber lines), 648, 683–685
 - DSS (Deliver, Service and Support) domain in COBIT 2019, 189
 - DSS (Digital Signature Standard), 352, 357
 - DSSS (direct sequence spread spectrum), 562–563
 - dual-attached concentrators (DACs)
 - in FDDI, 498
 - dual-attachment stations (DASs)
 - in FDDI, 498
 - dual control, 34
 - dual-homed firewalls, 959, 963
 - dual-use goods, 145
 - due care issues
 - disaster recovery plans, 1060
 - liability, 158–159
 - due diligence, 158–159
 - dumpster diving, 260–261
 - Dunn, Andy, 885
 - durability in ACID properties, 286
 - duress codes, 931–932
 - Dutch Data Protection Authority, 397
 - DVR (digital video recording)
 - systems, 913
 - Dyn attack, 307
 - dynamic analysis
 - antimalware software, 970
 - application security, 1139
 - dynamic application security testing (DAST), 1139
 - Dynamic Frequency Selection (DFS), 574
 - Dynamic Host Configuration Protocol (DHCP)
 - IP addresses, 501
 - overview, 517–519
 - dynamic mapping in NAT, 532
 - dynamic passwords, 729–732
 - dynamic ports, 507
 - dynamic routing protocols, 534–535
 - dynamic separation of duty (DSD)
 - relations, 773
 - Dyre Trojan, 604
- ## E
- E-carriers for WANs, 542
 - e-discovery, 236–237
 - e-mail
 - authorization, 624
 - DKIM, 625
 - DMARC, 625
 - gateways, 663
 - IMAP, 623–624
 - MIME, 625–626
 - overview, 621–622
 - phishing, 864
 - POP, 623
 - SPF, 624
 - threats, 623
 - E2EE (end-to-end encryption) vs. link encryption, 600–602
 - EAC (electronic access control) tokens, 925

- EAP (Extensible Authentication Protocol)
 - VPNs, 699
 - WPA Enterprise, 577
- EAP and Transport Layer Security (EAP-TLS), 580–581
- EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) authentication framework, 501
- EAP-Tunneled Transport Layer Security (EAP-TTLS), 580
- ECC (elliptic curve cryptography), 328, 342–343
- Economic Espionage Act, 141
- economic wrongs category in civil law, 128
- edge computing systems, 308–309
- EDI (electronic data interchange), 538
- EDLP (endpoint DLP), 273–274
- EDM (Evaluate, Direct and Monitor) domain in COBIT 2019, 189
- EDNS(0) technique in DNS, 620
- EDR. *See* endpoint detection and response (EDR)
- EDRM (Electronic Discovery Reference Model), 237
- EDU domain in DNS, 527
- education. *See* training
- EF (exposure factor), 74
- effectiveness monitoring for risk, 91–92
- egress
 - filtering, 948
 - monitoring, 981
- 80/20 Pareto principle, 179
- 802.1AE standard, 500–501
- 802.1AR standard, 501
- 802.1x standard, 579–581
- 802.11 standard, 565–566, 575–576
- 802.11a standard, 566–567
- 802.11ac standard, 567
- 802.11ax standard, 567–568
- 802.11b standard, 566
- 802.11e standard, 573
- 802.11f standard, 574
- 802.11g standard, 567
- 802.11h standard, 574
- 802.11i standard, 576–578
- 802.11j standard, 574
- 802.11n standard, 567
- 802.11w standard, 578
- 802.15.4 standard, 570–571
- 802.16 standard, 569
- EIGRP (Enhanced Interior Gateway Routing Protocol), 536
- EKs (endorsement keys) in Trusted Platform Modules, 405
- Elastic Stack product, 979
- electric power
 - backup, 448–450
 - considerations, 438
 - fallback plans, 448
 - issues, 450–452
 - overview, 670–672
 - protecting, 452–453
- electrical wires in transmission media, 643
- electromagnetic analysis for smart cards, 735
- electromagnetic interference (EMI)
 - coaxial cable, 649
 - electric power, 450
- electromechanical IDSs, 926
- electronic access control (EAC) tokens, 925
- electronic data interchange (EDI), 538
- Electronic Discovery Reference Model (EDRM), 237
- electronic monitoring of passwords, 721
- electronic vaulting for backups, 1038–1039
- electronically stored information (ESI), 236–237
- elevation of privilege category in STRIDE model, 388
- elliptic curve cryptography (ECC), 328, 342–343
- embedded systems, 306
- Embedding Business Continuity practice in Good Practice Guidelines, 105
- emergency category in PACE plans, 1057
- emergency changes, 892
- emergency management, 931
- emergency response groups, 1057
- emergency response procedures, 868–869
- EMI (electromagnetic interference)
 - coaxial cable, 649
 - electric power, 450
- Emotet Trojan, 604
- employees. *See* personnel safety and security
- emtocells in Li-Fi standard, 568
- emulating services in honeypots, 974
- emulation buffers in antimalware, 970

- Encapsulating Security Payload (ESP), 608
- encapsulation
 - multilayer protocols, 628
 - object-oriented programming, 1127–1128, 1130
 - OSI, 472–473
 - TCP, 509
- encryption. *See also* cryptology
 - bus, 407–408
 - code repositories, 1144
 - data at rest, 255
 - data in motion, 255–256
 - homomorphic, 258
 - hybrid methods, 346–350
 - Internet of Things, 307
 - Kerberos, 785–789
 - link vs. end-to-end encryption, 600–602
 - meeting applications, 694
 - mobile devices, 243
 - network sockets, 703
 - overview, 256–258
 - passwords, 722
- end-of-life (EOL) of assets, 229
- end-of-support (EOS) of assets, 229
- end-to-end encryption (E2EE) vs. link encryption, 600–602
- end-user environment in business continuity planning, 1071
- End User License Agreement (EULA), 153
- endorsement keys (EKs) in Trusted Platform Modules, 405
- endpoint detection and response (EDR)
 - breach attack simulations, 828
 - defense in depth, 391
 - effectiveness monitoring, 91–92
 - HIDSs, 968
 - security operations centers, 940
- endpoint DLP (EDLP), 273–274
- endpoint security, 673–674
- Enhanced Interior Gateway Routing Protocol (EIGRP), 536
- Enhanced Performance Architecture (EPA), 627
- Enigma machine, 320
- ENISA (European Union Agency for Cybersecurity), 106
- enrollment in biometric authentication, 725
- enterprise architecture frameworks
 - military-oriented, 195–196
 - models, 172–173
 - need for, 191–192
 - overview, 189–191
 - The Open Group Architecture Framework, 194–195
 - Zachman Framework, 192–194
- enterprise security architecture
 - description, 13
 - vs. ISMS, 26
- enterprise security program in business continuity management, 106–108
- entry points in physical security, 439–441
- enumeration step in penetration testing, 824
- environmental issues
 - business continuity planning, 1071
 - CPTED, 427–433
 - digital asset management, 262
 - disaster recovery, 1059
 - site and facilities, 461
- Environmental Protection Agency (EPA), 434
- EOL (end-of-life) of assets, 229
- EOS (end-of-support) of assets, 229
- EPA (Enhanced Performance Architecture), 627
- EPA (Environmental Protection Agency), 434
- ephemeral keys in TLS, 604
- ephemeral ports, 507
- equipment malfunction in risk management, 54
- equipment warranty, 672
- erasing media, 259
- escrow, software, 1070, 1143
- ESI (electronically stored information), 236–237
- ESMTP (Extended SMTP), 622
- ESP (Encapsulating Security Payload), 608
- ESTABLISHED state in TCP connections, 951
- Ethernet
 - data link layer, 481–482
 - layer 2 protocol, 494–495
 - local area networks, 499
 - Metro Ethernet, 539–540
 - Token Ring, 495–496

- ethics
 - professional, 44–46
 - vulnerability disclosures, 872
 - EULA (End User License Agreement), 153
 - European Union Agency for Cybersecurity (ENISA), 106
 - European Union Laws, 142–144
 - Evaluate, Direct and Monitor (EDM) domain in COBIT 2019, 189
 - evaluation
 - business impact analysis, 110–112
 - change management procedure, 891
 - framework steps, 201
 - program effectiveness, 43–44
 - Everything as a Service (XaaS), 304–305
 - evidence
 - acquiring, 1012
 - admissibility, 1013–1014
 - collecting, 1008–1012
 - identification guidelines, 1009–1010
 - incident investigations, 1006–1007
 - order of volatility, 1016
 - preserving, 1013
 - storage, 447–448
 - evolution of attacks, 134–138
 - evolutionary prototypes in software development, 1096
 - examination stage in forensics investigations, 1016–1017
 - exception handling, 871
 - executive succession planning, 1043
 - executive summaries in reports, 872–875
 - executives
 - incident notifications for, 1004
 - risk reporting for, 94–95
 - roles, 19–22
 - exercises for disaster recovery plans, 1061–1062
 - exigent circumstances, 1011
 - exploitation
 - Cyber Kill Chain model, 388, 994
 - penetration testing, 824
 - exploratory methodology in software development, 1104
 - exposure, defined, 9
 - exposure factor (EF), 74
 - extended detection and response (XDR)
 - platforms, 968
 - Extended SMTP (ESMTP), 622
 - Extended TACACS (XTACACS), 790–791
 - extended teams in incident response plans, 1000–1001
 - Extensible Access Control Markup Language (XACML), 781
 - Extensible Authentication Protocol (EAP)
 - VPNs, 699
 - WPA Enterprise, 577
 - Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) authentication framework, 501
 - Extensible Markup Language (XML), 615, 777
 - exterior lighting, 911–912
 - exterior routing protocols, 536–537
 - external audits, 842–843
 - external labeling in digital asset management, 263
 - external parties issues in data loss prevention, 267
 - external perimeter security
 - bollards, 910–911
 - fencing, 908–910
 - lighting, 911–912
 - overview, 906–908
 - surveillance devices, 913
 - visual recording devices, 913–916
 - extranets, 537–538
 - Extreme Programming (XP), 1102
- ## F
- Facebook breach, 20
 - facial scans, 728
 - Facilitated Risk Analysis Process (FRAP), 68
 - facilities. *See* site and facility security
 - facility safety officers, 434
 - Factor Analysis of Information Risk (FAIR)
 - framework, 172, 179
 - factors in ISO/IEC 27004, defined, 852
 - fail-safe devices, 931
 - fail safe systems for locks, 921
 - failed logon attempts, 721–723
 - failing securely
 - network security, 598
 - secure design, 396–397
 - site and facility security, 422
 - third-party connectivity, 706
 - web services, 612

- failover capability in quality of service, 1051
- Failure Modes and Effect Analysis (FMEA), 69–71
- FAIR (Factor Analysis of Information Risk) framework, 172, 179
- fairness issue in forensics investigation interviews, 1019
- false acceptance rate (FAR) in biometric authentication, 724–725
- false negatives in anomaly-based IDS/IPS, 967
- false positives in anomaly-based IDS/IPS, 967
- false rejection rate (FRR) in biometric authentication, 724–725
- FAR (false acceptance rate) in biometric authentication, 724–725
- FAST (Federation Against Software Theft), 154
- fault generation attacks on smart cards, 734
- fault injection attacks in cryptography, 372
- fault tolerance in availability, 1051
- fault tree analysis in risk assessment, 71–72
- FCoE (Fibre Channel over Ethernet) protocol, 628–629
- FCS (frame check sequence) numbers in WANs, 546
- FDDI (Fiber Distributed Data Interface) technology, 496–499
- FDDI rings in MANs, 538
- FDE (full-disk encryption), 407
- FDM (frequency-division multiplexing), 544
- FDMA (frequency division multiple access), 584
- Federal Copyright Act, 149–150
- Federal Emergency Management Agency (FEMA), 1054
- Federal Information Processing Standard (FIPS) 140-2, 406–407
- Federal Risk and Authorization Management Program (FedRAMP), 156, 1146
- Federal Rules of Evidence (FRE), 1014
- federated identity management (FIM) systems
 - overview, 752–754
 - with third-party service, 754–756
- Federation Against Software Theft (FAST), 154
- FedRAMP (Federal Risk and Authorization Management Program), 156, 1146
- Feistel, Horst, 332
- FEMA (Federal Emergency Management Agency), 1054
- fencing, 908–910
- FHSS (frequency hopping spread spectrum), 561–563
- Fiber Distributed Data Interface (FDDI) technology, 496–499
- fiber-optic cable, 650–651
- Fibre Channel over Ethernet (FCoE) protocol, 628–629
- field kits for digital forensics, 1015
- field of view in CCTV systems, 913, 915
- fifth-generation (5G) mobile wireless, 586–587
- fifth-generation programming languages, 1119–1120
- file descriptor attacks, 821
- file permissions, 821
- File Transfer Protocol (FTP)
 - application-level proxies, 954
 - sessions, 951
- filters
 - DNS, 621
 - firewalls. *See* firewalls
 - QKD, 344–345
- FIM (federated identity management) systems
 - overview, 752–754
 - with third-party service, 754–756
- FIN-WAIT-1 state in TCP connections, 951
- FIN-WAIT-2 state in TCP connections, 951
- findings in reports, 873
- finances for executive management, 20
- fingerprint detection in antimalware software, 969
- fingerprints, 726
- FIPS (Federal Information Processing Standard) 140-2, 406–407
- fire codes for door placement, 440
- fire detection considerations, 438
- fire extinguishers, 455
- fire prevention, 454
- fire rating for cabling, 653
- fire resistance ratings, 456
- fire-resistant material, 439
- fire safety
 - detection, 454–457
 - overview, 454

- fire sensors, 445
- fire suppression
 - considerations, 438
 - fire types, 458–459
 - heat-activated, 456–457
 - overview, 454, 457–459
 - smoke activated, 456
 - water sprinklers, 459–460
- firewalls
 - appliances, 958
 - architecture, 959–965
 - bastion hosts, 965
 - comparisons, 958
 - configuring, 965–966
 - demilitarized zones, 945–946
 - dual-homed, 959
 - next-generation, 957–958
 - overview, 945–946
 - packet-filtering, 946–949
 - proxy, 952–957
 - screened host, 959–960
 - screened subnet, 960–962
 - stateful, 949–952
 - virtual, 964
- first-generation (1G) mobile wireless, 585–586
- first-generation programming languages, 1118
- five nines availability, 1050
- fixed focal length in CCTV systems, 914–915
- fixed mounting cameras in CCTV systems, 916
- floods, SYN, 508
- flooring considerations, 438
- fluorescent lighting interference, 450
- FMEA (Failure Modes and Effect Analysis), 69–71
- foams for fire suppression, 459
- focal length in CCTV systems, 914–915
- foot-candles
 - CCTV systems, 916
 - lighting, 911
- footprints of satellites, 589
- forensics. *See* digital forensics
- Forrester report, 1134
- forward secrecy in TLS, 604
- forwarding planes in SDNs, 633–634
- forwarding proxies, 663–664
- forwarding tables for bridges, 656–657
- Foundational controls, 187
- Fourth Amendment issues, 1011
- fourth-generation (4G) mobile wireless, 586–587
- fourth-generation programming languages, 1119–1120
- fractional T lines, 542
- fragmentation in firewalls, 948, 965–966
- frame check sequence (FCS) numbers in WANs, 546
- frame relay for WANs, 547–548, 552
- frames
 - description, 483
 - packets, 509
 - TCP, 509
- Framework Core, 182–183
- Framework Profile in Cybersecurity Framework, 182
- frameworks
 - chapter questions, 205–209
 - chapter review, 203–205
 - CIS controls, 185–187
 - CMM, 197–199
 - COBIT 2019, 187–189
 - description, 15
 - enterprise architecture, 189–196
 - information security, 179–189
 - ITIL, 196–197
 - overview, 171–173
 - process steps, 199–203
 - risk, 172–179
 - security controls, 183–189
 - security programs, 180–183
 - Six Sigma, 197
- framing risk, 57
- Franklin, Benjamin, 317
- FRAP (Facilitated Risk Analysis Process), 68
- fraud
 - IP telephony, 692
 - PBX systems, 666
- FRE (Federal Rules of Evidence), 1014
- free space transmission media, 644
- freeware, 153
- frequency analysis attacks in cryptography, 370
- frequency division multiple access (FDMA), 584
- frequency-division multiplexing (FDM), 544

- frequency hopping spread spectrum (FHSS), 561–563
- frequency in wireless signals, 559
- FRR (false rejection rate) in biometric authentication, 724–725
- FTP (File Transfer Protocol)
 - application-level proxies, 954
 - sessions, 951
- full backups, 1035–1036
- full-disk encryption (FDE), 407
- full-duplex
 - session layer, 478
 - TCP, 508
- full-interruption tests in disaster recovery plans, 1064
- full knowledge in penetration testing, 825
- full RBAC, 773
- full tunnels in VPNs, 697
- functional analysis in BIA, 109
- functional model in software development design, 1084
- functional policies, 28
- functional requirements in software development, 1083
- fuzzing in application security testing, 1139–1140

G

- G.fast standard, 684
- gamification, 42–43
- garbage collectors in programming languages, 1122
- gas lines, 438
- gatekeepers in H.323, 689
- gates, 910
- gateways
 - characteristics, 665
 - H.323, 689
- gauge for fencing, 909
- General Data Protection Regulation (GDPR)
 - compliance monitoring, 93
 - entities, 143–144
 - FIM systems, 754
 - legal systems, 126
 - privacy issues, 147, 158, 397
- general hierarchies in RBAC, 772
- General Personal Data Protection Law, 144
- Generalized Markup Language (GML), 776

- generators, 449–450
- Generic Routing Encapsulation (GRE), 606
- Geneva, Switzerland, QKD in, 346
- geosynchronous satellites, 588–590
- GET methods in HTTP, 614
- Get Out of Jail Free Cards, 824
- glare protection, 912
- glass in data processing facilities, 446
- Glenny, Misha, 939
- Global System for Mobile Communication (GSM), 584
- GML (Generalized Markup Language), 776
- goals
 - audits, 839
 - disaster recovery, 1053–1054
- GOC domain in DNS, 527
- Gold Masters, 225
- Good Practice Guidelines (GPG), 105–106
- Goodman, Marc, 597
- Google trademark case, 150
- governance committees, 18
- Governance function in SAMM, 1109
- governance objectives in COBIT 2019, 189
- governance, risk, and compliance (GRC)
 - programs, 155
- GPG (Good Practice Guidelines), 105–106
- grades of locks, 923
- Graham-Denning model, 402–403
- Gramm-Leach-Bliley Act, 141, 147
- gray box testing, 826
- GRC (governance, risk, and compliance)
 - programs, 155
- GRE (Generic Routing Encapsulation), 606
- Gretzky, Wayne, 997
- groups for separation of duties, 394
- GSM (Global System for Mobile Communication), 584
- guaranteed service in QoS, 551
- Guaranteed Time Slot (GTS) reservations in WPANs, 570
- guards, 928–929
- guests in virtualized systems, 296
- guidelines
 - coding, 1136
 - overview, 32
- Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 142–144

H

- H.323 standard, 689
- HA (high availability), 1050–1053
- HaaS (Hacking as a Service), 135
- hacking mobile phones, 588
- hacktivists, 61
- Hadnagy, Chris, 902
- HAIPE (High Assurance Internet Protocol Encryptor), 609
- half-duplex mode in session layer, 478
- hand geometry, 727
- hand topography, 728–729
- handling evidence, 1008–1015
- handoffs in 802.11f standard, 574
- handouts for information access control, 801
- handshakes
 - RADIUS, 789
 - session keys, 350
 - SIP, 689–690
 - SSH, 700–701
 - TCP, 508, 949–951
 - TLS, 603
- hardware
 - backups in business continuity planning, 1069–1070
 - cryptography systems, 602
 - electrical power, 670–672
 - operation, 670–672
 - supply chain risk management, 98
 - tracking, 224
- hardware guard in MAC, 770
- hardware reverse engineering in cryptography, 371
- hardware security modules (HSMs), 406–407
- Harrison-Ruzzo-Ullman (HRU) model, 402–404
- hash chaining, 831
- hash MAC (HMAC), 355, 358
- hashing functions
 - algorithms, 351–352
 - attacks against, 353
 - overview, 351
 - passwords, 722
- HDLC (High-level Data Link Control) frames, 550
- headers
 - IPv6, 513–514
 - TCP, 950–951
- Health Information Technology for Economic and Clinical Health (HI-TECH) Act, 141
- Health Insurance Portability and Accountability Act (HIPAA), 147
- hearsay evidence, 1014
- Heartbleed security bug, 257, 370
- heat-activated fire suppression, 456–457
- heating, ventilation, and air conditioning (HVAC)
 - considerations, 438
 - data processing facilities, 446
 - fire suppression, 459
 - overview, 453–454
- heavy timber construction material, 439
- heavyweight methods in software development, 1101
- Hellman, Martin, 337–340
- Hello messages in TLS, 603
- help desk tasks and responsibilities, 886
- heuristic detection in antimalware software, 969, 971
- hexadecimal values, 1121
- HI-TECH (Health Information Technology for Economic and Clinical Health) Act, 141
- hiding data in steganography, 264–265
- HIDSs (host-based intrusion detection systems), 967
- hierarchical RBAC, 772–773
- hierarchical storage management (HSM) for backups, 898–899
- High Assurance Internet Protocol Encryptor (HAIPE), 609
- high availability (HA), 1050–1053
- high coupling in software, 1131–1132
- High-level Data Link Control (HDLC) frames, 550
- high-level languages, 1118–1121
- high-performance computing (HPC) systems, 288–289
- high privacy risk in software development, 1082
- High-Speed Serial Interface (HSSI), 552
- Hinckley, Gordon B., 171
- hints for passwords, 720
- HIPAA (Health Insurance Portability and Accountability Act), 147
- hiring candidates, 35–36
- history of changes, documenting, 262

- HMAC (hash MAC), 355, 358
 - HMI (human-machine interface), 291–294
 - holistic risk management, 54–55
 - hollow-core doors, 440
 - home IP address in mobile IP, 793
 - homomorphic encryption, 258
 - honeyclients, 975
 - honeynets, 975
 - honeypots, 974–976
 - hop devices, 601
 - hop sequences in FHSS, 561–563
 - Hopper, Grace, 851
 - hopping attacks in VLANs, 632
 - horizontal enactment for privacy, 147
 - host addresses in IP addresses, 510
 - host-based intrusion detection systems (HIDSs), 967
 - hostage alarm feature for combination locks, 920
 - HOSTS file in DNS, 528, 530
 - hosts in virtualized systems, 296
 - hot sites
 - disaster recovery, 1044–1046
 - vs. redundant sites, 1049
 - hot washes
 - event debriefing, 869
 - lessons learned, 1061
 - hotel key cards, 921
 - HPC (high-performance computing) systems, 288–289
 - HR (human resources)
 - disasters, 1042–1043
 - proofing of identity, 739
 - HRU (Harrison-Ruzzo-Ullman) model, 402–404
 - HSM (hierarchical storage management) for backups, 898–899
 - HSMs (hardware security modules), 406–407
 - HSSI (High-Speed Serial Interface), 552
 - HTML (Hypertext Markup Language), 776–777
 - HTTP (hypertext transfer protocol), 613–614
 - HTTPS (Hypertext Transfer Protocol Secure), 614
 - hubs, 655–656
 - human interaction in risk management, 54
 - human-machine interface (HMI), 291–294
 - human resource managers on incident response teams, 1001
 - human resources (HR)
 - disasters, 1042–1043
 - proofing of identity, 739
 - human sensors for incident detection, 995
 - human vulnerabilities, 902–903
 - humidity
 - data processing facilities, 446
 - HVAC systems, 453
 - hygrometers, 461
 - HVAC. *See* heating, ventilation, and air conditioning (HVAC)
 - hybrid clouds, 305
 - hybrid controls in Risk Management Framework, 175
 - hybrid data loss prevention, 274
 - hybrid encryption methods, 346
 - asymmetric and symmetric together, 346–349
 - session keys, 349–350
 - hybrid FIM systems, 756
 - hybrid flow in OIDC, 784
 - hybrid RBAC, 773
 - hybrid smart cards, 734
 - hybrid teams for incident response, 991
 - hygrometers, 461
 - Hypertext Markup Language (HTML), 776–777
 - hypertext transfer protocol (HTTP), 613–614
 - Hypertext Transfer Protocol Secure (HTTPS), 614
 - hypervisors in virtual machines, 296–298
- ## I
- IaaS (Infrastructure as a Service), 228, 302, 304
 - IAM (identity and access management), 745
 - ICMP. *See* Internet Control Message Protocol (ICMP)
 - ICSs. *See* industrial control systems (ICSs)
 - ICVs (Integrity Check Values), 501, 575–576
 - IDaaS (Identity as a Service), 754
 - IDC (International Data Corporation), 154
 - identification, 214
 - authentication. *See* authentication
 - credential management, 736–745
 - crime scenes, 1009–1010

- ul style="list-style-type: none;">
- identification (*cont.*)
 - description, 716
 - directory services, 747–750
 - FIM systems, 752–754
 - forensics investigations, 1016–1017
 - identity management, 745–754
 - life cycle of assets, 222–223
 - proofing, 738–740
 - single sign-on, 750–752
- identify function in Framework Core, 182
- identities and access fundamentals
 - access control and markup languages, 776–781
 - authorization. *See* authorization
 - chapter questions, 759–763
 - chapter review, 756–758
 - overview, 715–717
 - remote access control, 789–795
- identity and access management (IAM), 745
 - attribute-based access control, 774
 - authorization. *See* authorization
 - chapter questions, 805–809
 - chapter review, 804–805
 - discretionary access control, 766–768
 - life cycle management, 795–800
 - mandatory access control, 768–771
 - overview, 765
 - physical and logical access, 801–803
 - provisioning life cycle, 795–800
 - risk-based access control, 775–776
 - role-based access control, 771–773
 - rule-based access control, 774
- Identity as a Service (IDaaS), 754
- identity-based access control, 767
- identity management (IdM)
 - directory roles, 748–750
 - directory services, 747–748
 - federated identity management systems, 752–754
 - federated identity with third-party services, 754–756
 - overview, 745–747
 - single sign-on, 750–752
- identity providers (IdPs)
 - OpenID Connect, 783
 - SAML, 780
- identity repositories, 739
- identity stores, 748
- IDEs (integrated development environments)
 - in software development, 1137
- iDevIDs (initial device identities), 501
- IDFs (intermediate distribution facilities), 446–447
- IdPs (identity providers)
 - OpenID Connect, 783
 - SAML, 780
- IDSs. *See* intrusion detection systems (IDSs)
- IEC (International Electrotechnical Commission) 27000 Series, 180–182
- IETF (Internet Engineering Task Force) RFC 4987, SYN flood attacks, 508
- if this, then that (IFTTT) programming rules, 774
- IGMP (Internet Group Management Protocol), 500
- IGP (Interior Gateway Protocol), 533
- IGRP (Interior Gateway Routing Protocol), 536
- IGs (implementation groups) in CIS controls, 187
- IIoT (Industrial Internet of Things) devices, 570
- IKE (Internet Key Exchange), 608
- illogical processing, 62
- illumination in CCTV systems, 913, 916
- images
 - evidence, 1012–1013
 - system, 896
- IMAP (Internet Message Access Protocol), 623–624
- impact in incidents classification, 1002
- implementation
 - change management, 892
 - cybersecurity governance, 32–33
 - data loss prevention, 270–271
 - disaster recovery goals, 1054
 - frameworks, 200
 - Good Practice Guidelines, 106
 - Risk Management Framework, 175–176
 - SAMM, 1109
 - software, 1133
- implementation attacks in cryptography, 370–372
- implementation groups (IGs) in CIS controls, 187
- Implementation Tiers in Cybersecurity Framework, 182

- implicit denies in firewalls, 965
- implicit flow in OIDC, 784
- import/export controls for data breaches, 145–146
- IMPs (incident management policies), 990, 1000
- IMSI (International Mobile Subscriber Identity) catchers, 588
- in-rush current for electric power, 451
- inactivity, session termination from, 741
- incident assessment in site planning, 424
- incident investigations
 - chapter questions, 1024–1027
 - chapter review, 1022–1024
 - digital forensics, 1015–1022
 - evidence collection and handling, 1008–1015
 - law enforcement involvement, 1007
 - motive, opportunity, and means, 1007–1008
 - overview, 1006–1007
 - privacy issues, 1014
- incident management in business continuity, 1066
- incident management policies (IMPs), 990, 1000
- incident responders, tasks and responsibilities, 886
- incident response plans (IRPs)
 - classifications, 1002–1003
 - notifications, 1003–1004
 - operational tasks, 1004–1005
 - overview, 1000
 - roles and responsibilities, 1000–1002
 - runbooks, 1006
- incidents
 - classification, 1002–1003
 - Cyber Kill Chain framework, 994–995
 - detection, 995–996
 - investigations. *See* incident investigations
 - lessons learned, 999–1000
 - management overview, 989–994
 - mitigating, 996–997
 - notifications, 1003–1004
 - operational tasks, 1004–1005
 - overview, 989
 - recovery, 998
 - remediating, 999
 - reporting, 997–998
 - response plans, 1000–1006
 - response teams, 991
 - responses, 996
 - runbooks, 1006
 - supply chain risk management, 100
- incombustible material, 439
- income approach for executive summaries, 874
- incomplete level in CMMI, 1107
- incremental backups, 1036–1037
- Incremental software development, 1096–1097
- incremental testing for federated identity, 755
- indexing for data retention, 236
- indicators in ISO/IEC 27004, 852
- indicators of attack (IOAs), 999
- indicators of compromise (IOCs)
 - incident remediation, 999
 - threat data sources, 942
- Individual Participation Principle in OECD, 142
- industrial control systems (ICSs)
 - devices, 291–293
 - distributed control systems, 293
 - overview, 289–290
 - SCADA systems, 294
 - security, 294–295
- Industrial Internet of Things (IIoT) devices, 570
- industrial, scientific, and medical (ISM) bands, 565–566
- industry standards, compliance with, 156–158
- inference in database systems, 287
- information disclosure category in STRIDE model, 388
- information security
 - access control, 801
 - bus encryption, 407–408
 - classification, 215–219
 - frameworks, 179–189
 - hardware security modules, 406–407
 - identification, 215–219
 - overview, 214, 404
 - secure processing, 408
 - self-encrypting drives, 407
 - trusted execution environments, 408–410
 - Trusted Platform Modules, 404–406
 - vulnerabilities, 59

- Information Security Continuous Monitoring (ISCM), 981–982
- information security management
 - systems (ISMSs)
 - commercial software certifications, 1146
 - description, 12
 - vs. enterprise security architecture, 26
 - ISO/IEC 27000 series, 180
 - security operations centers, 939
- Information Systems Audit and Control Association (ISACA), 187
- information systems availability in business continuity planning, 1067–1070
- information systems risk management (ISRM)
 - policies, 56
- information systems view (Tier 3) in risk management, 55
- Information Technology Infrastructure Library (ITIL), 196–197
- informational model in software development design, 1084
- informative policies, 30
- Infrastructure as a Service (IaaS), 228, 302, 304
- infrastructure WLANs, 565
- ingress filtering, 948
- initial level in CMMI, 1107
- initial device identities (iDevIDs), 501
- initialization vectors (IVs)
 - 802.11 standard, 575–576
 - symmetric key cryptography, 334–335
- inputs, reviewing, 876–877
- inside attacks in risk management, 54
- installation stage in Cyber Kill Chain model, 388, 994
- instantiation in object-oriented programming, 1125
- INT domain in DNS, 527
- integrated development environments (IDEs)
 - in software development, 1137
- integrated product teams (IPTs), 1105
- Integrated Services Digital Network (ISDN), 685–686
- integration issues in federated identity, 754–755
- integration testing in software development, 1091
- integrity
 - Biba model, 399
 - CIA triad, 8
 - in cryptography, hashing functions, 351–354
 - in cryptography, message verification, 354–358
 - in cryptography, overview, 351
 - cryptosystems, 323
 - overview, 5–6
- Integrity Check Values (ICVs), 501, 575–576
- integrity verification procedures (IVPs) in Clark-Wilson model, 400
- Intel trade secrets theft, 149
- intellectual property (IP)
 - data breaches, 139
 - internal protection, 152–153
 - requirements. *See* licensing and intellectual property requirements
- intelligence cycle in threat intelligence, 941–942
- intentional category in civil law, 127
- interface testing, 837
- interference
 - coaxial cable, 649
 - electric power, 450–451
 - twisted-pair cabling, 649–650
- Interior Gateway Protocol (IGP), 533
- Interior Gateway Routing Protocol (IGRP), 536
- interior routing protocols, 535–536
- intermediate distribution facilities (IDFs), 446–447
- Intermediate System to Intermediate System (IS-IS), 536
- internal actors, 61–62
- internal audits, 840–842
- internal labeling in digital asset management, 263
- internal partitions, 442
- internal protection of intellectual property, 152–153
- internal security controls, 924
- internal sources of threat data, 942–943
- International Data Corporation (IDC), 154
- International Electrotechnical Commission (IEC) 27000 Series, 180–182
- international issues in cybercrimes, 138–139

- International Mobile Subscriber Identity (IMSI) catchers, 588
- International Organization for Standardization (ISO)
 - ISO 7498-1, 472
 - ISO 22301:2019, 105–106
 - ISO 28000:2007, 224
 - ISO/IEC 14443, 735
 - ISO/IEC 27000 series, 172, 180–182
 - ISO/IEC 27001, 1146
 - ISO/IEC 27004, 852
 - ISO/IEC 27005, 177–179
 - ISO/IEC 27031:2011, 105–106
 - ISO/IEC 27034, 1146
 - ISO/IEC 27037, 1009
 - network reference model, 470
- Internet Control Message Protocol (ICMP)
 - attacks using, 520–522, 537
 - message types, 520–521
 - overview, 520
 - stateful firewalls, 952
- Internet Engineering Task Force (IETF) RFC 4987, SYN flood attacks, 508
- Internet Group Management Protocol (IGMP), 500
- Internet growth, increase of attacks from, 134
- Internet Key Exchange (IKE), 608
- Internet Message Access Protocol (IMAP), 623–624
- Internet of Things (IoT)
 - devices, 570
 - issues, 306–307
- Internet Protocol (IP)
 - addresses. *See* IP addresses
 - L2TP, 606–607
- Internet protocol networking
 - ARP, 515–517
 - DHCP, 517–519
 - DNS, 524–531
 - ICMP, 520–522
 - IP addresses, 510–515
 - NAT, 531–533
 - overview, 502–503
 - routing protocols, 533–537
 - SNMP, 522–524
 - TCP, 503–509
- Internet Protocol Security (IPSec)
 - transport adjacency, 609
 - VPNs, 607–609
- Internet Protocol telephony, 687–688
 - H.323, 689
 - issues, 692
 - SIP, 689–691
- Internet Security Association and Key Management Protocol (ISAKMP), 608
- Internet Small Computer Systems Interface (iSCSI), 629
- internetworks, 657
- interoperability
 - data loss prevention, 270
 - ISO/IEC 14443, 735
- interpreters, 1119–1122
- interviews in forensics investigations, 1018–1019
- Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), 514
- intranets, 537–538
- intraorganizational configuration in SIP, 691
- intrasite tunneling mechanisms, 514
- intrusion detection systems (IDSs)
 - anomaly-based, 967–968
 - audits, 743
 - characteristics, 928
 - dogs, 929
 - overview, 925–928, 967
 - patrol forces and guards, 928–929
 - physical security, 908
 - rule-based, 967
 - whitelisting and blacklisting, 968–969
- intrusion prevention systems (IPSs)
 - anomaly-based, 967–968
 - overview, 967
 - rule-based, 967
 - whitelisting and blacklisting, 968–969
- inventories
 - data loss prevention, 267–268
 - digital asset management, 262
 - hardware, 224
 - software, 224–227
- investigations
 - incidents. *See* incident investigations
 - requirements, 161–162
- INVITE messages in SIP, 689–690
- invocation property in Biba model, 399
- IOAs (indicators of attack), 999

- IOCs (indicators of compromise)
 - incident remediation, 999
 - threat data sources, 942
 - IoT (Internet of Things)
 - devices, 570
 - issues, 306–307
 - IP addresses
 - DHCP, 501
 - DNS, 524–531
 - multicasting, 500
 - NAT, 531–533
 - overview, 510–512
 - packet-filtering firewalls, 948
 - three-way-handshake process, 951
 - IP convergence, 628
 - IP (intellectual property)
 - data breaches, 139
 - internal protection, 152–153
 - requirements. *See* licensing and intellectual property requirements
 - IP (Internet Protocol)
 - addresses. *See* IP addresses
 - L2TP, 606–607
 - networking, 502–503
 - IP version 4 (IPv4), 510
 - IP version 6 (IPv6), 510, 512–514
 - IPSec (Internet Protocol Security)
 - transport adjacency, 609
 - VPNs, 607–609
 - IPTs (integrated product teams), 1105
 - IPv4 (IP version 4), 510
 - IPv6 (IP version 6), 510, 512–514
 - iris lenses in CCTV systems, 915–916
 - iris scans, 727
 - IRPs. *See* incident response plans (IRPs)
 - IS-IS (Intermediate System to Intermediate System), 536
 - ISACA (Information Systems Audit and Control Association), 187
 - ISAKMP (Internet Security Association and Key Management Protocol), 608
 - ISATAP (Intra-Site Automatic Tunnel Addressing Protocol), 514
 - (ISC)² Code of Ethics, 44–45
 - ISCM (Information Security Continuous Monitoring), 981–982
 - iSCSI (Internet Small Computer Systems Interface), 629
 - ISDN (Integrated Services Digital Network), 685–686
 - island-hopping attacks, 133
 - ISM (industrial, scientific, and medical)
 - bands, 565–566
 - ISMSs. *See* information security management systems (ISMSs)
 - ISO. *See* International Organization for Standardization (ISO)
 - isochronous networks, 687
 - isolation in ACID properties, 286
 - ISRM (information systems risk management)
 - policies, 56
 - issue-specific policies, 28
 - IT engineers, tasks and responsibilities, 886
 - IT Governance Institute (ITGI), 187
 - IT support specialists on incident response teams, 1001
 - iterated tunneling in IPSec, 609
 - ITGI (IT Governance Institute), 187
 - ITIL (Information Technology Infrastructure Library), 196–197
 - IVPs (integrity verification procedures) in Clark-Wilson model, 400
 - IVs (initialization vectors)
 - 802.11 standard, 575–576
 - symmetric key cryptography, 334–335
- ## J
- JAD (Joint Application Development), 1104–1105
 - Java programming language, 1121–1122
 - bytecode, 1122–1123
 - protection mechanisms, 1123–1124
 - Java Virtual Machine (JVM), 1122–1123
 - JavaScript Object Notation (JSON), 615
 - JavaScript programming language, 1121
 - Jigsaw ransomware, 604
 - JIT (just-in-time) access, 738
 - jitter in IP telephony, 687–688
 - job rotation, 34, 889–890
 - Joint Application Development (JAD), 1104–1105
 - journaling, remote, 1039
 - JSON (JavaScript Object Notation), 615
 - jumbograms in IPv6, 514
 - jump boxes, 700

jurisdiction in incident response, 993
just-in-time (JIT) access, 738
JVM (Java Virtual Machine), 1122–1123

K

k-means clustering, 978
k-nearest neighbors (KNN), 977
Kanban development methodology,
1102–1103
KBA (knowledge-based authentication)
description, 718
passwords, 720–723
KDCs (Key Distribution Centers)
Kerberos, 785–788
PKI, 365
Kelling, George L., 433
Kerberos protocol
authentication process, 785–788
components, 785
key management, 365
overview, 784–785
passwords, 789
weaknesses, 788–789
Kerckhoffs, Auguste, 324–325
Kerckhoffs' principle, 324–325
kernel flaws in cryptography, 819
key distillation in quantum
cryptography, 344
Key Distribution Centers (KDCs)
Kerberos, 785–788
PKI, 365
key escrow in PKI, 366
key exchange protocol in RSA, 340
key management in PKI, 364–367
key override feature for combination
locks, 920
key performance indicators (KPIs),
155, 856–857
key risk indicators (KRIs), 855–857
keycard entry systems, 442
keys
asymmetric key cryptography, 335
cryptography, 322–323, 367–370
Diffie-Hellman algorithm, 337–338
hybrid methods, 347–348
RSA, 340–341
session, 349–350
symmetric key cryptography, 329

TLS, 604
ZigBee, 572
keyspaces for cryptology, 322
keystream generators in symmetric key
cryptography, 333
keystroke dynamics, 728
kill chains in threat modeling, 386
kill switches in VPNs, 697
knowledge-based authentication (KBA)
description, 718
passwords, 720–723
known-plaintext attacks in cryptography, 368
Koolhaas, Rem, 417
KPIs (key performance indicators), 155,
856–857
KRIs (key risk indicators), 855–857

L

L2F (Layer 2 Forwarding) protocol, 606
L2TP (Layer 2 Tunneling Protocol),
606–607
labels
digital asset management, 263
evidence, 1010
IPv6, 514
MAC, 768–769
laminated windows, 441
landscaping, 908
language in reports, 871
LANs. *See* local area networks (LANs)
LAST-ACK state in TCP connections, 951
last full backups, 1035–1036
latency in cabling, 654
law enforcement involvement in incident
investigations, 1007
laws and regulations
data breaches, European Union, 142–144
data breaches, U.S., 141–142
legal systems, 126–130
overview, 125–126
security programs, 434
layer 2
local area networks, 494–499
security standards, 500–502
Layer 2 Forwarding (L2F) protocol, 606
Layer 2 Tunneling Protocol (L2TP),
606–607
layer 3 and 4 switches, 659

- layers
 - encryption, 600–601
 - OSI reference model. *See* Open Systems Interconnection (OSI) reference model
- LDAP (Lightweight Directory Access Protocol), 747, 749
- LEAP (Lightweight Extensible Authentication Protocol), 580
- leased lines for WANs, 541–543
- least privilege principle
 - configuration management, 799
 - description, 888
 - endpoint security, 673
 - network security, 598
 - overview, 394–395
 - privileged accounts, 889
 - site and facility security, 421
 - software tracking, 225
 - third parties, 705–706
 - web services, 611
- least significant bits (LSBs) in steganography, 265
- LEDs (light-emitting diodes) in fiber-optic cable, 651
- legacy systems for federated identity, 755
- legal counsels in incident response teams, 1001
- legal departments, advice from, 157
- legal requirements
 - compliance, 156–158
 - physical security programs, 434
 - site planning, 427
- legal systems
 - civil law, 126, 129
 - common law, 126–130
 - customary law system, 128
 - mixed law system, 128–129
 - religious law system, 128
- legality issues in evidence admissibility, 1013–1014
- legally recognized obligations, 161
- Lei Geral de Proteção de Dados (LGPD), 144
- length of passwords, 720
- lenses in CCTV systems, 915–916
- LEO (low Earth orbit) satellites, 588–590
- lessons learned
 - disaster recovery plans, 1061
 - incidents, 999–1000
- levels
 - classification, 216–219
 - CMMI, 1107–1108
 - programming languages, 1120
- LGPD (Lei Geral de Proteção de Dados), 144
- Li-Fi standard, 568
- liability
 - civil law, 129
 - compliance, 158–161
 - outsourced security services, 974
- libraries
 - object-oriented programming, 1129–1130
 - software, 1132–1133
- licensing and intellectual property
 - requirements
 - copyrights, 149–150
 - internal protection of intellectual property, 152–153
 - overview, 147–148
 - patents, 151–152
 - software, 225–226
 - software piracy, 153–154
 - trade secrets, 148–149
 - trademarks, 150
- life cycle
 - business continuity planning, 1065–1067
 - cryptology, 328
 - data. *See* data life cycle
- life cycle of assets
 - decommissioning, 229–230
 - inventories, 224–227
 - overview, 222–223
 - ownership, 223
 - provisioning, 227–228
 - retention, 228–230
- life safety goals in site planning, 423
- light detectors in fiber-optic cable, 651
- light-emitting diodes (LEDs) in fiber-optic cable, 651
- light frame construction material, 438
- light sources for fiber-optic cable, 651
- lighting
 - CCTV systems, 916
 - EMI, 450
 - photoelectric IDSs, 926–927
 - physical security, 911–912
- Lightweight Directory Access Protocol (LDAP), 747, 749

- Lightweight Extensible Authentication Protocol (LEAP), 580
 - lightweight methods in software development, 1101
 - limited RBAC, 772–773
 - Linder, Doug, 1117
 - line conditioners for electric power, 451
 - line noise
 - cabling, 652
 - electric power, 450
 - line-of-succession plans, 1043
 - linear bus topology, 488
 - link encryption vs. end-to-end encryption, 600–602
 - link keys in ZigBee, 572
 - link-state routing protocols, 535
 - LISTEN state in TCP connections, 951
 - LLC (Logical Link Control), 481–482
 - loads, construction, 436
 - local area networks (LANs)
 - Ethernet, 494–495
 - FDDI, 496–498
 - medium access control, 489–494
 - protocols summary, 498–499
 - security standards, 500–502
 - Token Ring, 495–496
 - topologies, 487–490
 - transmission methods, 499–500
 - Local Security Authority Subsystem Service (LSASS), 372–374
 - Locard, Edmond, 1020
 - Locard's exchange principle, 1020–1021
 - lock bumping, 924
 - Lockheed Martin Cyber Kill Chain, 387–389
 - locks
 - administrative responsibilities, 922
 - circumventing, 922–924
 - grades, 923
 - mechanical, 918–922
 - overview, 917–918
 - Lucky ransomware, 604
 - logical access, 717, 801–803
 - logical acquisition of evidence, 1012
 - Logical Link Control (LLC), 481–482
 - logon attempts, failed, 721–723
 - logs
 - aggregating for microservices, 299
 - backups, 1039
 - evidence, 1014
 - managing, 978–979
 - protecting, 744–745
 - requirements factor, 978–979
 - reviews, 828–831
 - SIEM, 744, 979–980
 - standards, 979
 - tampering, 831
 - Long-Term Evolution (LTE), 587
 - loose coupling in software, 1131
 - loosely coupled microservices, 299
 - loss issues in risk management, 54, 63
 - low coupling in software, 1131
 - low Earth orbit (LEO) satellites, 588–590
 - low privacy risk in software development, 1083
 - LSASS (Local Security Authority Subsystem Service), 372–374
 - LSBs (least significant bits)
 - in steganography, 265
 - LTE (Long-Term Evolution), 587
 - Lucifer project, 321
 - lux values in CCTV systems, 916
- ## M
- m of n control
 - description, 34
 - PKI, 366–367
 - MAC (mandatory access control) model
 - characteristics, 776
 - overview, 768–771
 - MAC Security (MACSec) standard, 500–501
 - machine language, 1118, 1121
 - machine learning (ML), 977
 - MACSec Security Entity (SecY), 501
 - Madrid Agreement, 150
 - magnetic tapes for backups, 860
 - mail transfer agents (MTAs), 622
 - mailbox data, backups for, 862
 - main distribution facilities (MDFs), 446
 - maintenance
 - CPTED, 433
 - data, 238
 - frameworks, 201
 - maintenance hooks in software development, 1091
 - malicious code in advanced persistent threats, 136
 - malicious insiders, 61

- man-in-the-middle (MitM) attacks
 - cryptography, 374–375
 - data in motion, 59, 256
 - Diffie-Hellman algorithm, 338–339
- managed level in CMMI, 1107
- managed security services providers (MSSPs), 973–974
- managed service accounts (MSAs), 800
- managed services in software security, 1148
- Management Frame Protection (MFP), 578
- Management Information Base (MIB) in SNMP, 522–524
- management objectives in COBIT 2019, 189
- management review and approval, 875–877
- managers, risk reporting for, 95
- mandatory access control (MAC) model
 - characteristics, 776
 - overview, 768–771
- mandatory vacations, 35, 890
- manmade threats in site planning, 423
- MANs (metropolitan area networks), 538–540
- mantraps, 441
- manual iris lenses in CCTV systems, 915
- manual penetration tests (MPTs), 1140
- manual tests in software development, 1091
- market approach in executive
 - summaries, 874
- markup languages, 776–778
- Mary, Queen of Scots, 319
- masks in IP addresses, 511–512
- masquerading firewalls, 965
- master keying feature for combination locks, 920
- master keys in ZigBee, 572
- matrices
 - access control, 766–767
 - classification, 1002–1003
 - notification, 1003–1004
 - qualitative risk, 76–77
 - role, 799
- Mattermost service, 1057
- maturity models for risk, 96
- maturity software development models
 - CMMI, 1107–1109
 - overview, 1106
 - SAMM, 1109–1110
- MAUs (Multistation Access Units), 495
- maximum tolerable downtime (MTD)
 - BIA, 113–114
 - disaster recovery, 1030–1033
 - spare servers for, 672
- maximum tolerable period of disruption (MTPD), 113
- maximum transmission units (MTUs)
 - MAC mechanisms, 489–494
 - routers, 661
- “McAfee 2019 Cloud Adoption and Risk Report,” 303
- McNulty, Paul, 125
- MCUs (multipoint control units)
 - in H.323, 689
- MD5 (Message Digest 5)
 - description, 352
 - passwords, 722
- MDFs (main distribution facilities), 446
- MEA (Monitor, Evaluate and Assess) domain
 - in COBIT 2019, 189
- means in criminal investigations, 1008
- measurements in ISO/IEC 27004, 852
- measuring security, 851
 - account management, 858–860
 - backup verification, 860–862
 - chapter questions, 879–881
 - chapter review, 877–879
 - disaster recovery and business continuity, 867–869
 - key performance and risk indicators, 855–857
 - management review and approval, 875–877
 - metrics, 852–855
 - process data overview, 857–858
 - quantifying, 851–853
 - reporting, 869–875
 - training, 863–867
- mechanical locks, 918–922
- Media Access Control (MAC) addresses
 - ARP, 515–517
 - bridges, 656
 - DHCP, 519
 - switches, 658–659
- Media Access Control (MAC) in data link layer, 481–482
- media for storage, 447

- medium access control (MAC)
 - collision and broadcast domains, 492–494
 - CSMA, 490–491
 - overview, 489–490
 - polling, 494
 - token passing, 491–492
- meeting applications, 694–695
- Meltdown attacks, 257, 372
- members in object-oriented programming, 1125
- memory cards in ownership-based authentication, 732–733
- memory for Trusted Platform Modules, 405–406
- mergers and acquisitions (M&A), 17
- mesh size for fencing, 909
- mesh topology for local area networks, 488–489
- message authentication code (MAC), 355–356, 603–604
- Message Digest 5 (MD5)
 - description, 352
 - passwords, 722
- message digests, 354–355
- messages
 - ICMP, 520–521
 - integrity verification, 354–358
 - object-oriented programming, 1127–1128
 - TCP, 509
- meta-directories, 748
- methodologies
 - description, 15
 - reports, 873
- methods in object-oriented programming, 1127
- Metro Ethernet, 539–540
- metropolitan area networks (MANs), 538–540
- Metropolitan Transit Authority (MTA), 433
- MFA (multifactor authentication)
 - strong authentication, 719
 - VPNs, 697
- MFP (Management Frame Protection), 578
- MIB (Management Information Base) in SNMP, 522–524
- micro-segmentation, 629
- microcontrollers in embedded systems, 306
- microprobing attacks on smart cards, 735
- microservices, 299–301
- middle management, awareness
 - programs for, 42
- MIL domain in DNS, 527
- military-oriented architecture frameworks, 195–196
- Miller, Charlie, 627
- MIME (Multipurpose Internet Mail Extensions), 625–626
- MIMO (multiple input, multiple output)
 - standard, 567, 585
- Mirai botnet, 307
- mission/business process view (Tier 2) in risk management, 55
- mission critical data in disaster recovery, 1032
- misuse cases
 - data loss prevention, 271
 - testing, 835–836
- misuse of data in risk management, 54
- Mitchell, Joni, 213
- mitigation
 - incidents, 996–997
 - software security, 1144–1145
- mitigation risk strategy
 - ISO/IEC 27005, 178
 - overview, 79
- MitM (man-in-the-middle) attacks
 - cryptography, 374–375
 - data in motion, 59, 256
 - Diffie-Hellman algorithm, 338–339
- MITRE corporation
 - ATT&CK framework, 389–390
 - Common Weakness Enumeration initiative, 1088
- mixed law systems, 128–129
- ML (machine learning), 977
- MLS (multilevel security) systems
 - Bell-LaPadula, 398
 - description, 769
- MO (modus operandi) in criminal investigations, 1008
- mobile devices and communications
 - disaster recovery plans, 1062
 - endpoint security, 673–674
 - forensics investigations, 1021
 - generations, 585–587
 - hacking, 588

- mobile devices and communications (*cont.*)
 - multiple access technologies, 584–585
 - overview, 582–583
 - protecting, 220–221
- mobile hot sites in disaster recovery, 1049
- mobile IP, 793
- Modbus system, 627
- modems, cable, 686–687
- moderate privacy risk in software development, 1082
- modularity in object-oriented programming, 1127–1128
- modus operandi (MO) in criminal investigations, 1008
- MOM (motive, opportunity, and means) in incident investigations, 1007–1008
- Monitor, Evaluate and Assess (MEA) domain in COBIT 2019, 189
- monitoring
 - continuous, 981–982
 - egress, 981
 - frameworks, 201
 - ingress, 948
 - passwords, 721
 - Risk Management Framework, 176–177
 - UEBA, 981
- monitoring risk
 - change, 92–93
 - compliance, 93–94
 - continuous improvement, 95–96
 - description, 58
 - effectiveness, 91–92
 - maturity models, 96
 - reporting, 94–95
- monitors in Token Ring, 496
- monoalphabetic substitution ciphers, 318
- monoammonium phosphate for fire suppression, 458
- motion detectors, 927
- motive, opportunity, and means (MOM) in incident investigations, 1007–1008
- MPLS (Multiprotocol Label Switching)
 - Metro Ethernet, 540
 - routing tags and labels, 659
- MPTs (manual penetration tests), 1140
- MSAs (managed service accounts), 800
- MSSPs (managed security services providers), 973–974
- MTA (Metropolitan Transit Authority), 433
- MTAs (mail transfer agents), 622
- MTD (maximum tolerable downtime)
 - BIA, 113–114
 - disaster recovery, 1030–1033
 - spare servers for, 672
- MTPD (maximum tolerable period of disruption), 113
- MTUs (maximum transmission units)
 - MAC mechanisms, 489–494
 - routers, 661
- multi-user MIMO (MU-MIMO) technology, 567–568
- multicast transmission method, 499
- multifactor authentication (MFA)
 - strong authentication, 719
 - VPNs, 697
- multihomed devices, 959
- multilayer protocols, 626–627
- multilayered switches, 658
- multilevel security (MLS) systems
 - Bell-LaPadula, 398
 - description, 769
- multimedia collaboration, 693–694
 - meeting applications, 694–695
 - unified communications, 695–696
- multimode fiber-optic cable, 651
- multiparty key recovery in PKI, 366
- multiple access technologies in mobile communications, 584–585
- multiple input, multiple output (MIMO)
 - standard, 567, 585
- multiple processing sites in disasters recovery, 1049
- multiplexing functionalities, 544
- multipoint control units (MCUs) in H.323, 689
- Multiprotocol Label Switching (MPLS)
 - Metro Ethernet, 540
 - routing tags and labels, 659
- Multipurpose Internet Mail Extensions (MIME), 625–626
- Multistation Access Units (MAUs), 495
- muscle memory in disaster recovery, 1060
- mutual aid agreements in disasters recovery, 1047
- mutual authentication
 - description, 719
 - 802.11, 580

N

NAC (network access control)

devices, 667–668

importance, 697

namespaces

directory services, 747

DNS, 525

LDAP, 749

Nappo, Stephane, 989

NAS (network-attached storage) for

backups, 1038

NAT (network address translation),

512–513, 531–533

nation-state actors, 60–61

National Institute of Standards and Technology (NIST)

Cybersecurity Framework, 182

Digital Signature Standard, 357

enterprise architecture frameworks,

190–191

passwords, 720–721

Risk Management Framework, 172–177

SHA, 352

SP 800-30, 67–68, 173

SP 800-34, 104–105, 1059

SP 800-37, 173

SP 800-39, 55, 173

SP 800-53, 172, 175, 183–185

SP 800-57, 367

SP 800-60, 174

SP 800-63B, 720–721

SP 800-82, 290, 294

SP 800-88, 240

SP 800-111, 255

SP 800-137, 981–982

SP 800-161, 97

SP 800-190, 298–299

National Security Agency (NSA)

DES standard, 321

HAIPE, 609

natural access control in CPTED, 428–431

natural environmental threats in site

planning, 423

natural languages, 1119–1120

natural surveillance in CPTED, 431–432

natural threats, 62

naturalness in object-oriented

programming, 1127

NDAs (nondisclosure agreements)

incident response teams, 1001

trade secrets, 148

NDLP (network DLP), 272–273

NDR (network detection and response)

products

forensics investigations, 1021

HIDSs, 968

security operations centers, 940

Near Field Communication (NFC) with

smart cards, 735

near-line devices for backups, 898–899

need-to-know principle

description, 394

overview, 888

negligence

breaches from, 266

civil law category, 127

negligent insiders, 61

NET domain in DNS, 527

network access control (NAC)

devices, 667–668

importance, 697

network address translation (NAT),

512–513, 531–533

network administrators, tasks and

responsibilities, 886

network-attached storage (NAS) for

backups, 1038

network-based intrusion detection systems (NIDSs), 967

network components, 643

CDNs, 674

chapter questions, 677–679

chapter review, 674–676

devices. *See* network devices

endpoint security, 673–674

transmission media, 643–655

network detection and response (NDR)

products

forensics investigations, 1021

HIDSs, 968

security operations centers, 940

network devices

bridges, 656–657

gateways, 662–663

hardware operation, 670–672

NACs, 667–668

network diagramming, 668–670

- network devices (*cont.*)
 - overview, 655
 - PBXs, 665–667
 - proxy servers, 663–664
 - repeaters, 655–656
 - routers, 660–662
 - switches, 657–660
- network DLP (NDLP), 272–273
- network forensics, 1021
- network keys in ZigBee, 572
- network layer
 - functions and protocols, 484
 - OSI model, 480
- network reference models, 470–471
- network security
 - chapter questions, 638–641
 - chapter review, 635–638
 - design principles, 597–599
 - DNS, 616–621
 - e-mail, 621–626
 - link encryption vs. end-to-end encryption, 600–602
 - multilayer protocols, 626–627
 - overview, 597
 - protocol overview, 611
 - segmentation. *See* network segmentation
 - TLS, 602–605
 - VPNs, 605–611
 - web services, 611–616
- network segmentation
 - overview, 629
 - risk mitigation, 295
 - SD-WANs, 635
 - SDNs, 632–635
 - VLANs, 630–632
 - VxLANs, 632
- network sockets, 703
- Network Time Protocol (NTP), 829–830
- networking fundamentals
 - chapter questions, 555–558
 - chapter review, 552–555
 - data communications. *See* data communications
 - Internet protocol networking. *See* Internet protocol networking
 - intranets and extranets, 537–538
 - local area networks. *See* local area networks (LANs)
 - MANs, 538–540
 - overview, 469
 - WANs, 540–552
- networks
 - diagramming, 668–670
 - testing, 818
 - virtualized, 704–705
- New Zealand, Privacy Act in, 147
- newly observed domains (NODs) as threat data source, 943
- next-generation firewalls (NGFWs), 957–958
- NFC (Near Field Communication) with smart cards, 735
- NGFWs (next-generation firewalls), 957–958
- NIDSs (network-based intrusion detection systems), 967
- NIST. *See* National Institute of Standards and Technology (NIST)
- NMT (Nordic Mobile Telephone), 584
- NODs (newly observed domains) as threat data source, 943
- noise
 - cabling, 652
 - database systems, 288
 - digital transmission, 645
 - electric power, 450
- non-symbolic AI approach, 976–978
- nonces for one-time passwords, 731
- nondisasters
 - availability, 1049–1053
 - description, 1043
- nondisclosure agreements (NDAs)
 - incident response teams, 1001
 - trade secrets, 148
- nonfunctional requirements in software development, 1083
- noninterference model, 400–401, 403
- nonpersistent VDI, 701
- nonplenum cables, 653
- nonpracticing entities (NPEs), 152
- nonrecursive queries in DNS, 527
- nonrepudiation
 - cryptosystems, 324
 - overview, 6–7
- nonvolatile RAM (NVRAM) in Trusted Platform Modules, 405
- NORAD (North American Aerospace Defense Command), 436

- Nordic Mobile Telephone (NMT), 584
- normal changes, 892
- normal management in business
 - continuity, 1066
- normalization in data retention, 236
- North American Aerospace Defense Command (NORAD), 436
- notifications for incidents, 1003–1004
- Novell Red color, 150
- NPEs (nonpracticing entities), 152
- NSA (National Security Agency)
 - DES standard, 321
 - HAIPE, 609
- NTP (Network Time Protocol), 829–830
- nuisance category in civil law, 127
- NVRAM (nonvolatile RAM) in Trusted Platform Modules, 405
- O**
- O&M (operation and maintenance) in life cycle of assets, 223
- OASIS (Organization for the Advancement of Structured Information Standards), 781
- OAuth standard, 782–783
- Obama, Barack, 182
- object-oriented programming (OOP)
 - abstraction, 1129
 - benefits, 1127
 - classes and objects, 1125–1127
 - encapsulation, 1130
 - libraries, 1129–1130
 - messages, 1127–1128
 - overview, 1124–1125
 - vs. procedural programming, 1125–1126
 - relationships, 1128
- objectives in Spiral methodology, 1098
- objectivity in forensics investigation
 - interviews, 1019
- objects in ABAC, 774
- obligations, legally recognized, 161
- occupant emergency plans (OEPs), 931
- Occupational Safety and Health Administration (OSHA), 434
- OceanLotus attack, 389–390
- OCs (optical carriers) for WANs, 543
- OCSP (Online Certificate Status Protocol), 362
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) framework, 68, 172, 178–179
- OECD (Organisation for Economic Co-operation and Development), 142–144
- OEMs (original equipment manufacturers), 229
- OEPs (occupant emergency plans), 931
- OFDM (orthogonal frequency division multiplexing), 561, 563–564
- OFDMA (orthogonal frequency division multiple access), 585
- Office of Management and Budget, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information,” 140
- offline media for backups, 1038
- offsite backups, 1037
- offsite locations in disasters recovery, 1047
- OIDC (OpenID Connect), 783–784
- on-premise FIM systems, 755–756
- onboarding personnel security, 37–38
- ONC (Open Network Computing), 703
- one-time pads in cryptology, 325–328
- one-time passwords (OTPs), 729–732
- one-to-many identification, 718
- one-to-one identification, 718
- one-way hashing functions, attacks against, 353–354
- one-way RSA functions, 341–342
- ONF (Open Networking Foundation), 634–635
- online backups, 1035
- Online Certificate Status Protocol (OCSP), 362
- online encryption vs. end-to-end encryption, 600–602
- online safety, 866–867
- online UPS systems, 452–453
- onsite backups, 1037
- Ontario Information Commissioner, 397
- OOP. *See* object-oriented programming (OOP)
- open message format in asymmetric key cryptography, 336
- open network architectures, 472
- Open Network Computing (ONC), 703
- Open Networking Foundation (ONF), 634–635
- open proxies, 663

- Open Shortest Path First (OSPF) protocol, 535–536
- open-source intelligence (OSINT)
 - social engineering, 903
 - threat data sources, 942
- open-source software, securing, 1146–1147
- open system authentication (OSA), 575
- open systems, 474
- Open Systems Interconnection (OSI)
 - reference model, 470–471, 648
 - application layer, 474–475
 - attacks, 474
 - data link layer, 480–483
 - functions and protocols, 483–485
 - layers together, 485–487
 - network layer, 480
 - physical layer, 483
 - presentation layer, 475–476
 - protocols, 471–474
 - session layer, 477–478
 - transport layer, 479–480
- open trust model in ZigBee, 572
- Open Web Application Security Project (OWASP)
 - SAMM, 1109–1110
 - Threat Dragon, 1087
 - web applications, 1134–1135
- OpenFlow interface, 634–635
- OpenID Connect (OIDC), 783–784
- Openness Principle in OECD, 142
- operate steps in frameworks, 201
- operation and maintenance (O&M) in life cycle of assets, 223
- operational prototypes in software development, 1096
- operational tasks in incident handling, 1004–1005
- operational technology (OT), 290, 292–293, 295
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)
 - framework, 68, 172, 178–179
- operations and maintenance phase
 - change control, 1092–1094
 - change management, 1092
 - SDLC, 1080, 1091–1094
- Operations function in SAMM, 1109
- operations management. *See* security operations; security operations management
- opportunity in criminal investigations, 1008
- optical carriers (OCs) for WANs, 543
- optical discs for logs, 745
- optical fiber
 - fiber-optic cable, 651
 - transmission media, 643
- optical zoom in CCTV systems, 915
- optimizing level in CMMI, 1108
- orchestration in SOAR, 980
- order of volatility for evidence, 1016
- ORG domain in DNS, 527
- Organisation for Economic Co-operation and Development (OECD), 142–144
- Organization for the Advancement of Structured Information Standards (OASIS), 781
- organization view (Tier 1) in risk management, 55
- organizational change, data loss prevention in, 270
- organizational CIS controls, 187
- organizational code of ethics, 45
- organizational processes, 17–18
- organizational roles and responsibilities, 18–19
 - auditors, 25
 - change control analysts, 24
 - data analysts, 24
 - data custodians, 23
 - data owners, 22–23
 - executive management, 19–22
 - security administrators, 24
 - system owners, 23–24
 - users, 25
- organizational security policies, 27–29
- organizational units (OUs) in LDAP, 749
- organized cybercrime gangs, 134
- organizing steps for frameworks, 200
- original equipment manufacturers (OEMs), 229
- orthogonal frequency division multiple access (OFDMA), 585
- orthogonal frequency division multiplexing (OFDM), 561, 563–564
- OSA (open system authentication), 575
- OSHA (Occupational Safety and Health Administration), 434

OSI model. *See* Open Systems
Interconnection (OSI) reference model
OSINT (open-source intelligence)
 social engineering, 903
 threat data sources, 942
OSPF (Open Shortest Path First) protocol,
 535–536
OT (operational technology), 290,
 292–293, 295
OTPs (one-time passwords), 729–732
OUs (organizational units) in LDAP, 749
out-of-band method in symmetric key
 cryptography, 330
outside attacks in risk management, 54
outsourced security services, 973–974
outsourced software, 1147
outsourcing business continuity
 planning, 1068
overflows
 description, 819
 software development, 1089–1090
overlays in SDNs, 635
overwriting
 data, 243
 media, 259–260
OWASP (Open Web Application
 Security Project)
 SAMM, 1109–1110
 Threat Dragon, 1087
 web applications, 1134–1135
owners
 assets, 223
 data, 244
 OAuth, 782
 risk reporting for, 95
ownership-based authentication
 cryptographic keys, 732
 memory cards, 732–733
 one-time passwords, 729–732
 overview, 729
 smart cards, 733–735

P

PaaS (Platform as a Service), 228, 302–304
PACE (Primary, Alternate, Contingency, and
 Emergency) communications plans, 1057
package supplies in forensics field kits, 1015
packet-filtering firewalls, 946–949
packet jitter, 681
packet switching in WANs, 546–547
packets
 firewalls, 945
 TCP, 509
 TCP vs. UDP, 506
Padding Oracle On Downgraded Legacy
 Encryption (POODLE) attacks, 602
padlocks, 917
pair programming in Extreme
 Programming, 1102
palm scans, 727
PAM (privileged account management), 889
pan, tilt, or zoom (PTZ) capabilities in CCTV
 systems, 916
panic bars, 440
panic buttons, 931
PanOptis lawsuit, 151
PAP (Password Authentication Protocol),
 697–698
paper records, protecting, 221
parallel tests in disaster recovery plans, 1064
parameter validations in APIs, 1132
Pareto principle, 179
Paris Convention, 150
partial knowledge in penetration
 testing, 825
partitions
 database systems, 288
 physical security, 442
pass the hash attacks, 372
passive infrared (PIR) IDSs, 927
passive patch management, 904
passive relocking function for safes, 222
Password Authentication Protocol (PAP),
 697–698
password-guessing attacks, 789
password managers, 736–737
passwords
 checkers, 722
 cognitive, 723
 failed logon attempts, 721–723
 hashing and encrypting, 722
 Kerberos protocol, 789
 knowledge-based authentication, 720
 one-time, 729–732
 passphrases, 723
 PBX systems, 666

- passwords (*cont.*)
 - policies, 720–722
 - resets, 737–738
 - synchronization, 737
 - TACACS, 791
 - vulnerabilities, 60
- PAT (port address translation), 532
- patch management, 903
 - centralized, 904–905
 - reverse engineering patches, 905
 - unmanaged patching, 904
- patent trolls, 152
- patents, 151–152
- paths in URLs, 614
- patrol forces, 928–929
- payloads
 - IPv6, 514
 - steganography, 265
- PBXs (Private Branch Exchanges), 665–667
- PCI DSS (Payment Card Industry Data Security Standard), 156
- PCRs (platform configuration registers) in Trusted Platform Modules, 406
- PDC (Personal Digital Cellular), 584
- PDPA (Personal Data Protection Act), 144
- PDU (protocol data units)
 - description, 473
 - TCP, 509
- PEAP (Protected EAP), 580
- peer-to-peer systems, 307
- Peltier, Thomas, 68
- penetration tests
 - application security, 1140
 - knowledge of targets, 825–826
 - overview, 822–824
 - process, 824–825
 - red team exercises, 902
 - software development, 1090
 - vs. vulnerability tests, 826–827
- people as vulnerabilities, 60
- perfect forward secrecy in TLS, 604
- performance-based approach in site planning, 424
- performance metrics, 854
- Perimeter Intrusion Detection and Assessment System (PIDAS), 910
- perimeter security, 803
- periodic content reviews, 43
- peripheral switch controls for device locks, 921
- Perl programming language, 1121
- permanent teams for incident response, 991
- permanent virtual circuits (PVCs), 549
- permissions
 - DAC, 767
 - setting, 739
 - testing, 821
- persistent memory in Trusted Platform Modules, 405
- persistent VDI, 701
- Personal Data Protection Act (PDPA), 144
- Personal Digital Cellular (PDC), 584
- personal health information (PHI)
 - breaches, 255
- Personal Information Protection and Electronic Documents Act, 147
- personal liability of executive management, 20
- personally identifiable information (PII)
 - components, 140–141
 - U.S. laws, 141
- personnel
 - disaster recovery plans, 1055–1056
 - testing, 818
- personnel safety and security
 - access controls, 924–925
 - breaches from, 266
 - candidate screening and hiring, 35–36
 - compliance policies, 39–40
 - duress, 931–932
 - emergency management, 931
 - employment agreements and policies, 36–37
 - incident response, 993
 - onboarding, transfers, and termination processes, 37–38
 - overview, 33–35, 929–930
 - privacy policies, 40
 - threats, 138
 - training and awareness, 930–931
 - travel, 930
 - vendors, consultants, and contractors, 39
- perturbation in database systems, 288
- pervasive systems
 - embedded, 306
 - Internet of Things, 306–307
 - overview, 305

- Petya ransomware, 604
- PGP (Pretty Good Privacy), 367
- PHI (personal health information)
 - breaches, 255
- phishing awareness programs, 42, 864–865
- phone calls in PBXs, 665–667
- photoelectric IDS systems, 926–927
- phreakers, 666
- physical damage in risk management, 54
- physical destruction of data, 244
- physical layer
 - functions and protocols, 485
 - OSI model, 483
- physical security and controls
 - auditing, 929
 - data loss prevention, 269
 - devices, 802
 - digital asset management, 261
 - external perimeter, 906–916
 - facilities, 802–803, 916–924
 - information access, 801
 - internal controls, 924
 - intrusion detection systems, 925–929
 - mobile devices, 220–221
 - overview, 220, 801, 906
 - paper records, 221
 - personnel access controls, 924–925
 - risk responses, 83–84, 86–87
 - safes, 221–222
- physical security programs
 - construction, 436–439
 - design overview, 433–435
 - entry points, 439–441
 - facilities, 435–436
- physical surveillance in digital forensics, 1019–1020
- physical testing, 818
- physiological biometric authentication, 724
- PIDAS (Perimeter Intrusion Detection and Assessment System), 910
- piggybacking, 925
- PII (personally identifiable information)
 - components, 140–141
 - U.S. laws, 141
- pin tumbler locks, 918
- PINs
 - memory cards, 732
 - smart cards, 733
- PIR (passive infrared) IDSs, 927
- piracy, software, 153–154
- pirated software, dangers in, 225
- PKCS (Public Key Cryptography Standards), 626
- PKI. *See* public key infrastructure (PKI)
- plaintext, 321
- Plan-Do-Check-Act loop, 875
- plans
 - audits, 839
 - backups, 863
 - business continuity, 104–105
 - change management, 891
 - forensics investigation interviews, 1019
 - frameworks, 200
 - incident response, 1000–1006
 - OEPs, 931
 - Plan-Do-Check-Act loop, 875
 - Spiral methodology, 1098
- Platform as a Service (PaaS), 228, 302–304
- platform configuration registers (PCRs) in Trusted Platform Modules, 406
- platforms for secure software, 1137–1138
- PLCs (programmable logic controllers), 290–291
- plenum areas
 - cabling, 653
 - fire suppression, 459
- PMs (project managers) in software development, 1080
- point-to-point links in WANs, 541–543
- Point-to-Point Tunneling Protocol (PPTP), 606
- poisoning of ARP cache tables, 516–517
- polarized filters in QKD, 344–345
- policies
 - acceptable use, 226, 664, 858
 - compliance, 39–40
 - data retention, 234–236
 - employment, 36–37
 - IMPs, 990, 1000
 - passwords, 720–722
 - privacy, 40
 - security, 27–29
 - security operations centers, 940
 - types, 30

- Policy and Program Management
 - practice, 105
- policy engines for data loss prevention, 270
- polling, MAC, 494
- polyalphabetic substitution ciphers, 318–320
- polyvinyl chloride (PVC) jacket covering, 653
- POODLE (Padding Oracle On Downgraded Legacy Encryption) attacks, 602
- POP (Post Office Protocol), 623
- port address translation (PAT), 532
- portable code, 1122
- portable fire extinguishers, 455
- portals, TLS, 610
- portlets for web portal functions, 753–754
- ports
 - device locks, 921
 - packet-filtering firewalls, 948
 - TCP, 504
 - three-way-handshake process, 951
 - types, 507
- positive drains, 448
- POST methods in HTTP, 614
- Post Office Protocol (POP), 623
- powders for fire suppression, 458
- power, electrical. *See* electric power
- power supplies
 - considerations, 438
 - data processing facilities, 446
- PP (Professional Practices) in Good Practice Guidelines, 105–106
- PPTP (Point-to-Point Tunneling Protocol), 606
- preaction water sprinkler systems, 460
- prediction with artificial intelligence tools, 977
- prefabricated buildings in disasters
 - recovery, 1049
- preparation step
 - Risk Management Framework, 174
 - software vulnerability scans, 901
- preparedness metrics, 855
- presence information in unified communications, 695
- presentation layer
 - functions and protocols, 483–484
 - OSI model, 475–476
- presentation stage in forensics investigations, 1016–1018
- preservation
 - evidence, 1013
 - forensics investigations, 1016–1017
- preset locks, 917
- preshared keys (PSKs) in 802.11 standard, 575
- pressurized conduits for cabling, 653
- pretexting, 865
- Pretty Good Privacy (PGP), 367
- preventive and detective measures
 - anomaly-based intrusion detection and prevention, 967–968
 - antimalware software, 969–972
 - artificial intelligence tools, 976–978
 - firewalls. *See* firewalls
 - intrusion detection and prevention systems
 - overview, 967
 - outsourced security services, 973–974
 - process, 944–945
 - vs. recovery strategies, 1033
 - rule-based intrusion detection and prevention, 967
 - sandboxes, 972–973
 - whitelisting and blacklisting, 968–969
- preventive controls
 - business continuity, 104–105
 - risk responses, 85–87
- PRI (Primary Rate Interface) ISDN, 685–686
- Primary, Alternate, Contingency, and Emergency (PACE) communications plans, 1057
- primary category in PACE plans, 1057
- primary images for evidence, 1012
- Primary Rate Interface (PRI) ISDN, 685–686
- principals in KDC, 785
- principle of least privilege. *See* least privilege principle
- principles in SAML, 780
- priorities in disaster recovery goals, 1054
- privacy
 - classification level, 216–217
 - compliance issues, 147
 - control assessments, 90–91
 - data loss prevention, 270
 - incident investigations, 1014
 - policies, 40
 - requirements, 158
 - retina scan issues, 727
 - SDLC assessments, 1082
 - vs. security, 21

- privacy by design, 397
 - network security, 599
 - site and facility security, 423
 - third-party connectivity, 706
 - web services, 612
- Privacy by Design: Delivering the Promises* report, 397
- Private Branch Exchanges (PBXs), 665–667
- private clouds, 301, 305
- private keys
 - asymmetric key cryptography, 335
 - hybrid methods, 347
 - RSA, 340–341
- private portions in objects, 1128
- privilege escalation
 - identity and access, 799–800
 - software development, 1089
- privileged account management (PAM), 889
- PRNGs (pseudorandom number generators), 327, 370
- proactive searching in threat hunting, 943
- probationary periods in employment, 37
- procedural programming vs. object-oriented programming, 1125–1126
- procedures, 32
- process enhancement, 16
- process reengineering, 16
- processes
 - organizational, 17–18
 - race conditions, 717
 - vulnerabilities, 59–60, 902
- processing speed in biometric authentication, 726
- processors
 - data, 244–245
 - security extensions, 410
- professional ethics, 44–46
- Professional Practices for Business Continuity Management, 106
- Professional Practices (PP) in Good Practice Guidelines, 105–106
- profile updates, 740
- program effectiveness evaluation, 43–44
- programmable locks, 920
- programmable logic controllers (PLCs), 290–291
- programming languages and concepts.
 - See also* software development
 - assemblers, compilers, and interpreters, 1120–1122
 - levels, 1120
 - object-oriented programming, 1124–1130
 - overview, 1117–1120
 - runtime environments, 1122–1124
- Project Athena, 784
- project management in SDLC, 1081
- project managers (PMs) in software development, 1080
- project sizing factor in risk assessment, 64
- proofing of identity, 738–740
- protect function in Framework Core, 182
- Protected EAP (PEAP), 580
- protocol data units (PDUs)
 - description, 473
 - TCP, 509
- prototypes in software development, 1096
- provisioning
 - assets, 227–228
 - configuration management, 894–895
 - identity and access, 796
 - users, 739
- Provisioning Service Provider (PSP)
 - in SPML, 778
- Provisioning Service Target (PST)
 - in SPML, 778
- proximate causes, 161
- proximity detectors, 927
- proxy firewalls
 - application-level, 954–955, 957
 - circuit-level, 954–956
 - overview, 952–953
- proxy servers
 - characteristics, 665
 - overview, 663–664
 - SIP, 690
- pseudorandom number generators (PRNGs), 327, 370
- PSKs (preshared keys) in 802.11
 - standard, 575
- PSP (Provisioning Service Provider)
 - in SPML, 778
- PST (Provisioning Service Target)
 - in SPML, 778

- PSTNs (public switched telephone networks), 582–583, 682–683
- PTZ (pan, tilt, or zoom) capabilities in CCTV systems, 916
- public algorithms vs. secret, 369
- public classification level, 216–217
- public clouds, 301, 305
- public disclosure in incident response, 993
- public key cryptography, 328
- Public Key Cryptography Standards (PKCS), 626
- public key infrastructure (PKI)
 - certificate authorities, 360–362
 - code repositories, 1144
 - digital certificates, 359–360
 - key management, 364–367
 - overview, 359
 - registration authorities, 362
 - steps, 362–364
- public keys
 - asymmetric key cryptography, 335
 - hybrid methods, 347–348
 - RSA, 340–341
- public relations factor in incident response teams, 1001
- public switched telephone networks (PSTNs), 582–583, 682–683
- Purpose Specification Principle in OECD, 142
- PVC (polyvinyl chloride) jacket covering, 653
- PVCs (permanent virtual circuits), 549
- Python programming language, 1121–1122

Q

- QA (quality assurance) in software development, 1080
- QKD (quantum key distribution), 344
- QoS (Quality of Service)
 - ATM, 551–552
 - availability, 1050–1051
- qualitative risk analysis
 - description, 72
 - overview, 76–78
- quality, defined, 1117
- quality assurance (QA) in software development, 1080
- Quality of Service (QoS)
 - ATM, 551–552
 - availability, 1050–1051
- quantifiability of security metrics, 854
- quantifying security, 851–853
- quantitative risk analysis
 - description, 72
 - vs. qualitative, 78–79
 - results, 75–76
 - steps, 73–75
- quantitatively managed level in CMMI, 1108
- quantum cryptography, 344–346
- quantum key distribution (QKD), 344
- queries
 - DNS, 527–528, 616
 - URLs, 615
- quorum authentication
 - description, 34
 - PKI, 366–367

R

- RA (Requesting Authority) in SPML, 778
- race conditions
 - description, 821
 - processes, 717
- RAD (Rapid Application Development)
 - methodology, 1099–1100
- radio frequency interference (RFI)
 - electric power, 450
 - twisted-pair cabling, 649–650
- RADIUS (Remote Authentication Dial-In User Service)
 - network devices, 501
 - overview, 789–790
 - vs. TACACS, 791–793
- rainbow tables for passwords, 721–722
- raking locks, 922–923
- ramifications with compliance, 158–161
- random access memory (RAM) for Trusted Platform Modules, 405
- random numbers in cryptology, 327
- random password generation, 736
- random values in quantum cryptography, 345
- ransomware
 - cryptography, 375
 - protecting backups from, 897–898
 - TLS, 604
- Rapid Application Development (RAD)
 - methodology, 1099–1100
- rapid prototyping in software development, 1096

- RARP (Reverse Address Resolution Protocol), 519
- RAs (registration authorities), 360, 362
- RB-RBAC (rule-based access control), 774
- RBAC (role-based access control) model, 771
 - characteristics, 776
 - core, 772
 - hierarchical, 772–773
- RDP (Remote Desktop Protocol)
 - overview, 700
 - threat intelligence, 943
- RDS (Remote Desktop Services), 943
- reactive searching in threat hunting, 943
- real power, 671
- Real-time Transport Protocol (RTP), 689, 691
- real user monitoring (RUM) vs. synthetic transactions, 832
- realms in Kerberos, 785
- rebar, 439
- reciprocal agreements in disasters recovery, 1047–1048
- recommendations in reports, 873
- reconnaissance stage in Cyber Kill Chain model, 387, 994
- recording forensics investigation
 - interviews, 1019
- recover function in Framework Core, 182
- recovery
 - data loss prevention, 269
 - incidents, 998
 - risk responses, 85, 87
- recovery point objective (RPO)
 - disaster recovery, 1031–1032
 - high availability, 1052
- recovery strategies
 - availability, 1049–1053
 - business process recovery, 1033–1034
 - data backups, 1034–1041
 - documentation, 1041–1042
 - overview, 1029–1033
 - vs. preventive measures, 1033
 - reciprocal agreements, 1047–1048
 - recovery site strategies, 1043–1047
 - redundant sites, 1048–1049
- recovery teams in disaster recovery plans, 1056
- recovery time objective (RTO)
 - disaster recovery, 1031–1033
 - high availability, 1052
- rectilinear filters in QKD, 344
- recursive queries in DNS, 527, 616
- red teaming
 - exercises, 902
 - penetration tests, 827–828
- redirect servers in SIP, 691
- reduced-function devices (RFDs), 570
- reduction analysis in threat modeling, 386–387
- redundancy for quality of service, 1050–1051
- redundant lighting, 912
- redundant sites, 1048–1049
- REEs (rich execution environments), 408–409
- reference monitors, 766
- references for candidates, 37
- reflection attacks in DNS, 620
- registered ports, 507
- registered trademarks, 150
- registrar servers in SIP, 689–690
- registration authorities (RAs), 360, 362
- registration of accounts, 738–740
- regression analysis in artificial intelligence tools, 977
- regression testing in software development, 1091
- regulations. *See* laws and regulations
- regulatory investigation requirements, 162
- regulatory policies, 30
- reinforcing bar, 439
- relevance
 - evidence admissibility, 1013
 - security metrics, 854
- relevant characteristic in threat intelligence, 941
- reliability
 - disaster recovery, 1051–1052
 - evidence admissibility, 1013–1014
 - TCP vs. UDP, 506
- religious law system, 128
- relocation teams in disaster recovery plans, 1056
- relocking function for safes, 222
- remanence, data, 240–244
- remediate phase in software vulnerability scans, 901
- remediation
 - incidents, 999
 - vulnerabilities, 871

- remote access
 - desktop virtualization, 699–701
 - Diameter, 793–795
 - overview, 696, 789
 - RADIUS, 789–790
 - TACACS, 790–793
 - VPNs, 697–699
- Remote Authentication Dial-In User Service (RADIUS)
 - network devices, 501
 - overview, 789–790
 - vs. TACACS, 791–793
- Remote Desktop Protocol (RDP)
 - overview, 700
 - threat intelligence, 943
- Remote Desktop Services (RDS), 943
- remote desktops, 700
- remote journaling for backups, 1039
- remote logging, 831
- remote procedure calls (RPCs), 703–704
- remote terminal units (RTUs)
 - DNP3, 626
 - industrial controls, 290
 - SCADA systems, 294
- removal tools in forensics field kits, 1015
- repeaters
 - characteristics, 665
 - description, 655–656
- replay attacks
 - cryptography, 372–374
 - description, 787
- replication
 - backups, 1039–1040
 - logs, 831
- reports
 - digital forensics, 1021–1022
 - executive summaries, 872–875
 - incident response, 993
 - incidents, 997–998
 - overview, 869–870
 - penetration testing, 825
 - risk, 94–95
 - security results, 870–872
 - technical, 872–873
- repositories
 - backups, 1039
 - code, 1143–1144
 - identity, 739
- Representational State Transfer (REST), 615–616
- repudiation category in STRIDE model, 388
- reputation-based protection for antimalware software, 971
- reputation factor
 - disaster recovery, 1054
 - outsourced security services, 974
- request methods in HTTP, 614
- Requesting Authority (RA) in SPML, 778
- requests in change management, 891
- requirements gathering in SDLC, 1080, 1082–1083
- resets for passwords, 737–738
- residual risk vs. total risk, 81
- resilience
 - data loss prevention, 272
 - system, 1051
- resolvers in DNS, 527–528
- resource owners in OAuth, 782
- resource protection
 - backups, 896–899
 - overview, 895–896
 - source files, 896
 - system images, 896
- resource records in DNS, 525
- resource servers in OAuth, 782
- respond function in Framework Core, 182
- responses
 - disaster recovery plans, 1055
 - incidents, 996
 - physical security, 908
 - risk. *See* risk responses
 - site planning, 424
 - SOAR, 980
- responsibility
 - description, 161
 - disaster recovery goals, 1053
 - organizational. *See* organizational roles and responsibilities
- responsive area illumination, 912
- REST (Representational State Transfer), 615–616
- restoration
 - backups, 1037, 1041–1042
 - disaster recovery plans, 1058–1060
- restoration teams in disaster recovery plans, 1056

- restricted areas, 443
- results, analyzing, 870–872
- retention
 - assets, 228–230
 - data, 233–236
- retina scans, 727
- reusability in object-oriented programming, 1127
- reuse methodology in software development, 1105
- Reverse Address Resolution Protocol (RARP), 519
- reverse engineering attacks
 - in cryptography, 371
- reverse engineering patches, 905
- reverse proxies, 664
- reviews
 - audits, 743–744
 - change management, 892
- RFIDs (reduced-function devices), 570
- RFI (radio frequency interference)
 - electric power, 450
 - twisted-pair cabling, 649–650
- rich execution environments (REEs), 408–409
- right to be forgotten provision in GDPR, 144
- right to be informed provision in GDPR, 144
- right to restrict processing provision in GDPR, 144
- ring topology, 489
- RIP (Routing Information Protocol), 535
- risk
 - defined, 9
 - FAIR, 179
 - frameworks, 172–179
 - ISO/IEC 27005, 177–179
 - metrics, 854
 - OCTAVE, 178–179
 - Spiral methodology, 1098–1099
- risk analysis
 - qualitative, 72, 76–78
 - quantitative, 72–76, 78–79
 - software security, 1144–1145
- risk assessment
 - approaches, 72–76
 - asset valuation, 65–66
 - business impact analysis, 109–112
 - methodologies, 67–72
 - monitoring risk, 91–96
 - overview, 63–64
 - preventive and detective measures, 944
 - responses. *See* risk responses
 - SDLC, 1082–1083
 - teams, 66–67
- risk-based access control, 775–776
- risk-level acceptance in SDLC, 1082
- risk management
 - assessment. *See* risk assessment
 - business continuity. *See* business continuity (BC)
 - chapter questions, 118–123
 - chapter review, 116–118
 - concepts, 53–54
 - holistic, 54–55
 - information systems risk management
 - policy, 56
 - overview, 53
 - process, 57–58
 - risk analysis, 72–79
 - supply chain, 96–101
 - teams, 56–57
 - threats, 60–63
 - vulnerabilities, 58–60, 62–63
- Risk Management Framework, 172–177
- risk responses
 - control assessments, 88–91
 - control types, 83–88
 - countermeasure selection and implementation, 81–83
 - overview, 79–80
 - risk management response, 57
 - total risk vs. residual risk, 81
- Rivest, Ron, 340, 352
- roaming 802.11f standard, 574
- robustness of security metrics, 854
- role-based access control (RBAC) model, 771
 - characteristics, 776
 - core, 772
 - hierarchical, 772–773
- roles and responsibilities
 - data, 244–245
 - definitions, 799
 - incident response plans, 1000–1002
 - organizational. *See* organizational roles and responsibilities
 - separation of duties, 394
 - software development, 1080
 - tasks and responsibilities, 886

- rollback plans, 905
- rolling hot sites, 1049
- root account, 859
- round-trip time (RTT) in latency, 654
- route flapping, 535
- routers
 - vs. bridges, 657
 - characteristics, 665
 - overview, 660–662
- Routing Information Protocol (RIP), 535
- routing policies in BGP, 537
- routing protocols
 - attacks, 537
 - autonomous systems, 533–534
 - distance-vector vs. link-state, 535
 - dynamic vs. static, 534–535
 - exterior, 536–537
 - interior, 535–536
- RPC security (RPCSEC), 704
- RPCs (remote procedure calls), 703–704
- RPO (recovery point objective)
 - disaster recovery, 1031–1032
 - high availability, 1052
- RSA algorithm, 340–342
- RSA-CRT (Chinese Remainder Theorem), 372
- RSA SecurID, 730–732
- RTCP (RTP Control Protocol), 691
- RTEs (runtime environments), 1122–1124
- RTO (recovery time objective)
 - disaster recovery, 1031–1033
 - high availability, 1052
- RTP Control Protocol (RTCP), 691
- RTP (Real-time Transport Protocol), 689, 691
- RTT (round-trip time) in latency, 654
- RTUs (remote terminal units)
 - DNP3, 626
 - industrial controls, 290
 - SCADA systems, 294
- Ruff, Howard, 1029
- rule-based access control (RB-RBAC), 774
- rule-based IDS/IPS, 967
- rules in PKI key management, 366–367
- RUM (real user monitoring) vs. synthetic transactions, 832
- runbooks for incidents, 1006
- runtime environments (RTEs), 1122–1124

S

- S/MIME (Secure MIME), 626
- SaaS (Software as a Service), 228, 302–303
- SABSA (Sherwood Applied Business Security Architecture), 14–15, 173
- SACs (single-attached concentrators) in FDDI, 498
- Safe Harbor Privacy Principles, 143
- “Safeguarding Against and Responding to the Breach of Personally Identifiable Information,” 140
- safes, 221–222
- safety issues
 - disaster recovery, 1059
 - fires, 454–457
 - personnel. *See* personnel safety and security
- sags in electric power, 451
- salvage teams in disaster recovery plans, 1056
- SAML (Security Assertion Markup Language), 779–780
- SAMM (Software Assurance Maturity Model), 1109–1110
- sandboxes
 - antimalware, 969–970, 972–973
 - Java Virtual Machine, 1123
- sanitized media, 259
- Sarbanes-Oxley Act (SOX), 20
- SAs (security associations) in IPSec, 608
- SASL (Simple Authentication and Security Layer), 624
- SASs (single-attachment stations) in FDDI, 498
- SAST (static application security testing), 1139
- satellite communications, 589–590
- SCADA (supervisory control and data acquisition) systems, 290, 294
- scalability
 - Kerberos, 785
 - packet-filtering firewalls, 948
 - stateful firewalls, 952
- scans
 - devices, 226
 - facial, 728
 - iris, 727
 - palm, 727
 - retina, 727
 - software vulnerabilities, 901

- scenarios for backups, 863
- schemes in URLs, 613
- Schneier, Bruce, 385
- Scientific Working Group on Digital Evidence (SWGDE), 1009
- SCIFs (sensitive compartmented information facilities), 443
- SCM (software configuration management), 1142
- scope creep in project management, 1081
- scope of audits, 839
- scope values in OIDS, 784
- scoping controls, 258
- SCPs (service control points), 683
- screen sharing in meeting applications, 694
- screened host firewalls, 959–960, 963
- screened subnet firewalls, 960–962
- screening candidates, 35–36
- screens in information access control, 801
- script kiddies, 60, 135
- scrubbing logs, 744
- Scrum methodology, 1101–1102
- scytale ciphers, 318
- SD-WAN (software-defined wide area networking), 635
- SDLC. *See* software development life cycle (SDLC)
- SDN. *See* software-defined networking (SDN)
- sealing systems, 405
- second-generation (2G) mobile wireless, 585–586
- second-generation programming languages, 1118
- secondary storage in information access control, 801
- SecOps, 887
- secret algorithms vs. public, 369
- secret classification level, 216–218
- secret keys
 - hybrid methods, 348
 - RSA, 340–341
 - symmetric key cryptography, 329
- secure defaults
 - network security, 598
 - third-party connectivity, 706
 - web services, 611
- secure design principles, 390
 - defaults, 396
 - defense in depth, 390–391
 - failing securely, 396–397
 - least privilege, 394–395
 - privacy by design, 397
 - separation of duties, 393–394
 - shared responsibility, 392–393
 - simplicity, 395–396
 - trust but verify, 392
 - zero trust, 392
- secure enclaves in trusted execution environments, 408
- Secure Hash Algorithm (SHA)
 - description, 352
 - passwords, 722
- Secure MIME (S/MIME), 626
- Secure Shell (SSH)
 - code repositories, 1144
 - communications channels, 701–702
- secure software
 - acquired software, 1145–1148
 - APIs, 1132
 - application security testing, 1139–1140
 - assemblers, compilers, and interpreters, 1120–1122
 - assessments, 1144–1145
 - change management, 1145
 - chapter questions, 1150–1153
 - chapter review, 1148–1150
 - code repositories, 1143–1144
 - cohesion and coupling, 1130–1132
 - configuration management, 1142
 - continuous integration and delivery, 1140–1141
 - controls, 1136–1144
 - development platforms, 1137–1138
 - libraries, 1132–1133
 - object-oriented programming, 1124–1130
 - overview, 1117
 - programming languages and concepts, 1117–1120
 - risk analysis and mitigation, 1144–1145
 - runtime environments, 1122–1124
 - secure coding practices, 1134–1136
 - SOAR, 1141–1142
 - source code vulnerabilities, 1133–1134
 - tool sets, 1138

- security
 - aligning to business strategy, 13–16
 - assessments. *See* assessments
 - endpoint, 673–674
 - network. *See* network security
 - policies, 27–29
 - vs. privacy, 21
- security administrators, 24
- security architects, tasks and responsibilities, 886
- security architectures, 385
 - chapter questions, 413–416
 - chapter review, 411–413
 - encryption locations, 411
 - information systems, 404–410
 - secure design principles, 390–397
 - security models, 397–404
 - security requirements, 404
 - threat modeling, 385–390
- Security Assertion Markup Language (SAML), 779–780
- security associations (SAs) in IPSec, 608
- security champions, 43
- security controls. *See* controls
- security directors, tasks and responsibilities, 886
- security effectiveness in control
 - assessments, 90–91
- security film windows, 441
- security information and event management (SIEM) systems
 - event data, 831
 - forensics investigations, 1021
 - incidents, 990–991
 - logs, 744, 979–980
 - security operations centers, 940
- security managers, tasks and responsibilities, 886
- security models
 - Bell-LaPadula, 398–399
 - Biba, 399–400
 - Brewer and Nash, 402
 - Clark-Wilson, 400
 - Graham-Denning, 402
 - Harrison-Ruzzo-Ullman, 402–404
 - noninterference, 400–401
 - overview, 397–398
 - summary, 403
- security operations, 939
 - antimalware software, 969–972
 - artificial intelligence tools, 976–978
 - chapter questions, 984–988
 - chapter review, 982–984
 - firewalls. *See* firewalls
 - honeypots and honeynets, 974–976
 - intrusion detection and prevention systems
 - overview, 967–969
 - logging and monitoring, 978–982
 - outsourced security services, 973–974
 - preventive and detective measures overview, 944–945
 - sandboxes, 972–973
 - security operations centers, 939–943
- security operations centers (SOCs)
 - cyberthreat hunting, 943
 - elements, 940–941
 - overview, 939
 - threat data sources, 942–943
 - threat intelligence, 941–942
- security operations management, 885
 - accountability, 887–888
 - change management, 891–893
 - chapter questions, 934–938
 - chapter review, 932–934
 - configuration management, 893–895
 - foundational concepts overview, 885–887
 - job rotation, 889–890
 - need-to-know and least privilege, 888
 - patch management, 903–906
 - personnel safety and security, 929–932
 - physical security. *See* physical security and controls
 - privileged account management, 889
 - resource protection, 895–899
 - separation of duties and responsibilities, 888–889
 - service level agreements, 890
 - vulnerability management, 900–903
- security orchestration, automation, and response (SOAR) platform
 - components, 980
 - secure software, 1141–1142
- security programs in frameworks, 172, 180–183
- Security Safeguards Principle in OECD, 142
- security zones in CPTED, 429–430

- SecY (MACSec Security Entity), 501
- SEDs (self-encrypting drives), 407
- segmentation, network, 295, 703
- segments in TCP, 509
- SEI (Software Engineering Institute), 993
- select step in Risk Management Framework, 175
- self-encrypting drives (SEDs), 407
- self-healing SONEts, 539
- self-service
 - password resets, 737
 - profile updates, 740
- Sender Policy Framework (SPF), 624
- senior management, awareness
 - programs for, 41–42
- sensitive classification level, 216–217
- sensitive compartmented information facilities (SCIFs), 443
- sensitive data
 - classification, 215
 - data loss prevention, 266, 270
- sensors in incident detection, 995–996
- separation of duties (SoD) principle
 - network security, 599
 - overview, 888–889
 - purpose, 34
 - role-based access control, 773
 - security architectures, 393–394
 - site and facility security, 421
 - software development, 1090
 - third-party connectivity, 706
 - web services, 612
- sequels for tabletop exercises, 1063
- sequence numbers in TCP, 508
- server-based systems, 284–285
- serverless systems, 299–301
- servers
 - clustered, 1051
 - OAuth, 782
 - proxy, 663–664
- service availability risk from unmanaged patching threats, 904
- service bureaus in disaster recovery, 1045
- service control points (SCPs), 683
- service level agreements (SLAs)
 - high availability, 1050
 - overview, 890
 - supply chain risk management, 101
- service-oriented architecture (SOA)
 - description, 780–781
 - web services, 612–613
- Service Provisioning Markup Language (SPML), 777–779
- Service Set IDs (SSIDs), 565
- services in supply chain risk management, 99
- Session Initiation Protocol (SIP), 689–691
- session keys, 349–350
- session layer
 - functions and protocols, 484
 - OSI model, 477–478
- session management, 740–741
- severity levels for incidents, 1003
- SGML (Standard Generalized Markup Language), 776
- SHA (Secure Hash Algorithm)
 - description, 352
 - passwords, 722
- shallow depth of focus in CCTV systems, 915
- Shamir, Adi, 340
- Shannon, Claude, 332
- shared key authentication (SKA), 575
- shared portions in objects, 1128
- shared responsibility principle
 - network security, 599
 - security design, 392–393
 - site and facility security, 420–421
 - third-party connectivity, 706
 - web services, 612
- shareware, 153
- sharing data, 238–239
- Shedd, William G.T., 53
- Sherwood Applied Business Security Architecture (SABSA), 14–15, 173
- shielded twisted pair (STP) cable, 649
- Shkreli, Martin, 20
- Shortest Path Bridging (SPB) protocol, 657
- shoulder surfing, 5
- side-channel attacks
 - cryptography, 371–372
 - description, 257
 - smart cards, 734–735
- SIEM systems. *See* security information and event management (SIEM) systems
- signal switching points (SSPs), 682
- signal transfer points (STPs), 683
- Signaling System 7 (SS7) protocol, 682

- signature-based detection in antimalware software, 969, 971
- signature dynamics, 727–728
- signatures in antimalware software, 969
- Simple Authentication and Security Layer (SASL), 624
- simple integrity axiom in Biba model, 399
- Simple Mail Transfer Protocol (SMTP), 622
- Simple Network Management Protocol (SNMP), 522–524
- Simple Object Access Protocol (SOAP), 614–615, 780
- simple security rule in Bell-LaPadula, 398
- simplex communication, 831
- simplex mode in session layer, 478
- simplicity
 - network security, 599
 - secure design principles, 395–396
 - security metrics, 854
 - site and facility security, 422
 - third-party connectivity, 706
- Simpson, O.J., 129–130
- simulation tests in disaster recovery plans, 1064
- simulations for breach attacks, 828
- single-attached concentrators (SACs) in FDDI, 498
- single-attachment stations (SASs) in FDDI, 498
- single loss expectancy (SLE)
 - key risk indicators, 857
 - quantitative risk analysis, 73–75
- single mode in fiber-optic cable, 651
- single sign-on (SSO)
 - identity management, 750–752
 - replay attacks, 372–373
- SIP (Session Initiation Protocol), 689–691
- site and facility security
 - access control, 802–803
 - backups, 1040–1041
 - chapter questions, 463–465
 - chapter review, 461–462
 - controls. *See* controls for site and facilities
 - CPTED, 427–433
 - defaults, 422
 - defense in depth, 419
 - design overview, 417–418
 - least privilege, 421
 - locks, 917–923
 - overview, 417, 916–917
 - physical security programs, 433–441
 - planning steps, 423–427
 - principles, 418–423
 - privacy by design, 423
 - separation of duties, 421
 - shared responsibility, 420–421
 - simplicity, 422
 - threat modeling, 418–419
 - trust but verify, 420
 - zero trust, 419–420
- Site Security Design Guide*, 906
- situational awareness, 744
- 6to4 tunneling method, 514
- Six Sigma methodology, 197
- SKA (shared key authentication), 575
- Slack service, 1057
- SLAs (service level agreements)
 - high availability, 1050
 - overview, 890
 - supply chain risk management, 101
- SLE (single loss expectancy)
 - key risk indicators, 857
 - quantitative risk analysis, 73–75
- slot locks, 921
- smart cards
 - access codes, 921
 - attacks on, 734–735
 - ownership-based authentication, 733–735
- smart phones, 688
- smoke-activated fire suppression, 456
- smoke detectors, 445
- SMTP (Simple Mail Transfer Protocol), 622
- Smyth, Robin, 20
- SNMP (Simple Network Management Protocol), 522–524
- snooping in DHCP, 519
- Snowden, Edward, 62
- SOA (service-oriented architecture)
 - description, 780–781
 - web services, 612–613
- SOAP (Simple Object Access Protocol), 614–615, 780
- SOAR (security orchestration, automation, and response) platform
 - components, 980
 - secure software, 1141–1142

- social engineering
 - awareness programs, 42
 - cryptography attacks, 375
 - description, 5, 60
 - human vulnerabilities, 902–903
 - passwords, 721
 - training, 864–865
- social network vulnerabilities, 60
- sockets
 - description, 504
 - network, 703
- SOCKS proxy firewalls, 956
- SOCs. *See* security operations centers (SOCs)
- SoD principle. *See* separation of duties (SoD) principle
- soft controls for risk responses, 83
- soft tokens in one-time passwords, 732
- software
 - antimalware, 969–972
 - backups in business continuity planning, 1070
 - cryptography systems, 602
 - escrow, 1070, 1143
 - licensing, 226
 - meeting applications, 695
 - piracy, 153–154
 - secure. *See* secure software
 - smart card attacks, 735
 - supply chain risk management, 99
 - tracking, 224–227
 - vulnerabilities, 901
- Software as a Service (SaaS), 228, 302–303
- Software Assurance Maturity Model (SAMM), 1109–1110
- software configuration
 - management (SCM), 1142
- software-defined networking (SDN)
 - approaches, 634–635
 - control and forwarding planes, 633–634
 - overview, 632–633
 - secure software, 1136
- software-defined security (SDS), 1136
- software-defined wide area networking (SD-WAN), 635
- software developers, tasks and responsibilities, 886
- software development
 - Agile methodologies, 1100–1103
 - chapter questions, 1112–1116
 - chapter review, 1110–1111
 - cleanroom methodology, 1105
 - DevOps, 1103–1104
 - DevSecOps, 1104
 - exploratory methodology, 1104
 - Incremental methodology, 1096–1097
 - Joint Application Development
 - methodology, 1104
 - maturity models, 1106–1110
 - methodologies overview, 1095
 - methodologies summary, 1106
 - overview, 1079
 - prototypes, 1096
 - Rapid Application Development
 - methodology, 1099–1100
 - reuse methodology, 1105
 - roles, 1080
 - SDLC. *See* software development life cycle (SDLC)
 - Spiral methodology, 1098–1099
 - Waterfall methodology, 1095–1096
- software development life cycle (SDLC)
 - design phase, 1083–1087
 - development phase, 1087–1089
 - operations and maintenance phase, 1091–1094
 - overview, 1079–1080
 - phases summary, 1094
 - project management, 1081
 - requirements gathering phase, 1082–1083
 - testing phase, 1089–1091
- Software Engineering Institute (SEI), 993
- software engineers, 1080
- software guard in MAC, 770
- Software Requirements Specification (SRS), 1083
- solar window film windows, 441
- solid-core doors, 440
- something a person does authentication factor, 718
- something a person has authentication factor, 718–719
- something a person is authentication factor, 718
- something a person knows authentication factor, 718

- somewhere a person is authentication factor, 718
- SONETs (Synchronous Optical Networks), 538–539
- source code analysis attacks
 - in cryptography, 370
- source code vulnerabilities, 1133–1134
- source files, protecting, 896
- source routing in firewalls, 966
- Soviet Union collapse, increase of attacks from, 134
- SOW (statements of work) in project management, 1081
- SOX (Sarbanes-Oxley Act), 20
- Spafford, Eugene H., 3
- spaghetti code, 1126
- Spanning Tree Protocol (STP), 657
- SPB (Shortest Path Bridging) protocol, 657
- spearphishing, 865
- Specht, Paul, 150
- special characters in passwords, 720
- Spectre attacks, 257, 372
- speed
 - biometric authentication, 726
 - TCP vs. UDP, 506
- SPF (Sender Policy Framework), 624
- spikes in electric power, 451
- Spiral methodology for software development, 1098–1099
- split knowledge, 34
- split tunnels in VPNs, 697
- splitting DNS, 530
- Splunk product, 979
- SPML (Service Provisioning Markup Language), 777–779
- spoofing
 - e-mail, 623
 - firewalls, 965
 - STRIDE model, 388
- spread spectrum wireless communications, 561–563
- sprinklers, 459–460
- sprints in Scrum methodology, 1102
- SRKs (storage root keys) in Trusted Platform Modules, 405
- SRS (Software Requirements Specification), 1083
- SS7 (Signaling System 7) protocol, 682
- SSD (static separation of duty) relations in RBAC, 773
- SSH (Secure Shell)
 - code repositories, 1144
 - communications channels, 701–702
- SSIDs (Service Set IDs), 565
- SSO (single sign-on)
 - identity management, 750–752
 - replay attacks, 372–373
- SSPs (signal switching points), 682
- staff, awareness programs for, 42
- stakeholders
 - enterprise architecture frameworks, 190
 - incident notifications, 1004
- standalone mode in WLANs, 565
- standard changes, 892
- Standard Generalized Markup Language (SGML), 776
- standard windows, 441
- standards
 - business continuity, 104–106
 - coding, 1135–1136
 - controls, 258
 - industry, 156–158
 - logs, 979
 - organizational, 29–31
 - WLANs, 565–574
- standby lighting, 912
- standby UPS systems, 453
- star integrity axiom in Biba model, 399
- star property rule in Bell-LaPadula, 398
- star topology, 488
- start bits, 646
- state actors, 60–61
- state tables
 - stateful firewalls, 949, 952
 - three-way-handshake process, 951
- stateful firewalls, 949–952
- stateful NAT, 533
- stateless inspection in packet-filtering firewalls, 948
- statements of work (SOW) in project management, 1081
- states
 - controls, 254–258
 - TCP connections, 951
- static analysis
 - antimalware software, 970
 - application security, 1139

- static application security
 - testing (SAST), 1139
- static electricity, 454
- static mapping in NAT, 532
- static routing protocols, 534–535
- static separation of duty (SSD) relations
 - in RBAC, 773
- statistical attacks in cryptography, 370
- statistical time-division multiplexing (STDM), 544
- steganography, 264–265
- stegomedium, 265
- Stevens, Ted, 469
- sticky notes in Kanban methodology, 1102–1103
- Stoll, Clifford, 643
- stop bits, 646
- storage, data, 232–233, 259–260
- storage facilities, 447–448
- storage keys in Trusted Platform Modules, 406
- storage root keys (SRKs) in Trusted Platform Modules, 405
- STP (shielded twisted pair) cable, 649
- STP (Spanning Tree Protocol), 657
- STPs (signal transfer points), 683
- strata in NTP, 831
- strategic alignment, 15–16
- stream ciphers in symmetric key cryptography, 333–334
- stream-symmetric ciphers, 575
- streaming protocols, 691
- strict liability category in civil law, 128
- STRIDE model, 387–388
- strong authentication, 718–719
- strong star property rule in Bell-LaPadula, 398
- structured walkthrough tests in disaster recovery plans, 1063
- subjects
 - ABAC, 774
 - data, 245
- subnet masks in IP addresses, 511–512
- subnets in IP addresses, 510–512
- substitution ciphers, 318
- sub-techniques in MITRE ATT&CK framework, 389
- succession planning, 1043
- Sullivan, Joseph, 20
- supernetting IP addresses, 512
- supervisor role, 24
- supervisory control and data acquisition (SCADA) systems, 290, 294
- supply chain risk management
 - attacks, 133
 - hardware, 98
 - minimum security requirements, 100
 - overview, 96–98
 - risk sources, 99–100
 - service level agreements, 101
 - services, 99
 - software, 99
 - upstream and downstream, 98
- supply system threats in site planning, 423
- support agreements, 672
- support staff, tasks and responsibilities, 886
- surges in electric power, 451
- surveillance
 - CPTED, 431–432
 - description, 913
 - digital forensics, 1019–1020
- suspending accounts, 860
- sustain stage in change management, 892
- Sutter Health of California breach, 255
- SVCs (switched virtual circuits), 549
- SWGDE (Scientific Working Group on Digital Evidence), 1009
- swipe cards for ownership-based authentication, 732–733
- switch controls in device locks, 921
- switch spoofing attacks, 632
- switched virtual circuits (SVCs), 549
- switches
 - characteristics, 665
 - layer 3 and 4, 659
 - overview, 657–658
 - VLANs, 630
- switching WANs, 545–547
- symbolic AI approach, 976–978
- symbolic links, 819, 821
- symmetric key cryptography
 - with asymmetric, 346–349
 - block ciphers, 330–333
 - description, 328
 - initialization vectors, 334–335
 - overview, 329–330
 - stream ciphers, 333–334
 - summary, 330

- symmetric services in DSL, 684
- SYN/ACK packets, 508
- SYN floods, 508
- SYN packets, 508, 949–951
- SYN-RECEIVED state in TCP connections, 951
- SYN-SENT state in TCP connections, 951
- synchronization
 - NTP, 830
 - passwords, 737
- Synchronous Optical Networks (SONETs), 538–539
- synchronous replication, 1039
- synchronous token devices for one-time passwords, 730–731
- synchronous transmission, 645–647
- synthetic transactions, 832
- system access control, 802
- system account access review, 798
- system administrators, tasks and responsibilities, 886
- system architectures
 - chapter questions, 311–315
 - chapter review, 310–311
 - client-based, 284
 - cloud-based, 301–305
 - database, 285–286
 - distributed, 307–309
 - high-performance computing, 288–289
 - industrial control systems, 289–296
 - overview, 283
 - pervasive, 305–307
 - server-based, 284–285
 - virtualized systems, 296–301
- system authentication, 579
- system images, 896
- system-level event audits, 742
- system owners, 23–24
- system resilience in availability, 1051
- system sensing access control readers, 925
- system-specific controls in Risk Management Framework, 175
- system-specific policies, 29
- system testing, 818

T

- T-carriers for WANs, 541–542
- tables
 - forwarding, 656–657
 - rainbow, 721–722

- stateful firewalls, 949, 952
- three-way-handshake process, 951
- tabletop exercises (TTXs) in disaster recovery plans, 1063–1064
- TACACS (Terminal Access Controller Access Control System), 790–793
- TACS (Total Access Communication System), 584
- tactics in MITRE ATT&CK framework, 389
- tailoring controls, 258
- tamper-resistant property in reference monitors, 766
- tampering category in STRIDE model, 388
- tape vaulting for backups, 1039
- tapes for backups, 860
- Target company breach, 96–97
- target hardening vs. CPTED, 428
- targeted penetration tests, 826–827
- targets of attacks, 474
- tar pits, 976
- taxonomies in data retention, 236
- TCG (Trusted Computing Group), 404
- TCP. *See* Transmission Control Protocol (TCP)
- TCP/IP (Transmission Control Protocol/Internet Protocol) suite, 471, 502–503
- TDF (transborder data flow), 146–147
- TDM (time-division multiplexing), 541–542
- TDMA (time division multiple access)
 - GTS, 570
 - mobile communications, 584
- teams
 - backup administrators, 1035
 - business continuity planning, 1030
 - disaster recovery plans, 1056
 - incident response, 991, 1000–1001
 - risk analysis, 76, 78
 - risk assessment, 66–67
 - risk management, 56–57
 - software development, 1080
- technical controls
 - assessments. *See* testing
 - risk responses, 83, 86–87
- technical reports, 872–873
- technical sensors in incident detection, 995
- technological communication protocols, 646
- TEEs (trusted execution environments), 408–411
- telephone calls in PBXs, 665–667

- Telephone Records and Privacy Protection Act, 865
- telephones in disaster recovery plans, 1062
- telepresence in meeting applications, 695
- temperature
 - data processing facilities, 446
 - HVAC systems, 453–454
- tempered windows, 441
- templates for disaster recovery plans, 1059
- Temporal Key Integrity Protocol (TKIP), 577–578
- Teredo tunneling, 514
- Terminal Access Controller Access Control System (TACACS), 790–793
- terminals in H.323, 689
- termination processes in personnel security, 37–38
- territorial reinforcement in CPTED, 431–432
- tertiary sites in disaster recovery, 1046
- Tesla, Nikola, 559
- test coverage, 837
- test-driven development
 - Extreme Programming, 1102
 - software development, 1089
- testing
 - application security, 1139–1140
 - backups, 863
 - code reviews, 833–834
 - code testing, 834–835
 - compliance checks, 838
 - data loss prevention, 270–271
 - disaster recovery goals, 1054
 - disaster recovery plans, 1061–1065
 - federated identity, 755
 - interface, 837
 - log reviews, 828–831
 - misuse cases, 835–836
 - overview, 817
 - penetration, 822–827
 - red teaming, 827–828
 - SDLC, 1080, 1089–1091
 - Spiral methodology, 1098
 - strategies, 813–816
 - synthetic transactions, 832
 - test coverage, 837
 - vulnerabilities, 817–822
- testing mode in anomaly-based IDS/IPS, 967
- text messages in disaster recovery plans, 1056
- TGSs (ticket granting services) in KDC, 785–786
- Thailand, Personal Data Protection Act in, 144
- The Onion Router (TOR), 307
- The Open Group Architecture Framework (TOGAF), 172, 194–195
- The Silk Road, 665
- thermal relocking function in safes, 222
- third-generation (3G) mobile wireless, 585–586
- Third Generation Partnership Project (3GPP), 586
- third-generation programming languages, 1118–1119
- third parties
 - audits, 843–844
 - business continuity planning, 1068
 - connectivity, 705–706
 - dealing with, 39
 - security provided by, 973–974
 - software escrow, 1143
 - software security, 1147
- third-party sensors in incident detection, 995
- third-party services, federated identity with, 754–756
- threat data sources for security operations centers, 942–943
- Threat Dragon, 1087
- threat hunters, tasks and responsibilities, 886
- threat hunting in security operations centers, 943
- threat intelligence analysts on incident response teams, 1001
- threat intelligence in security operations centers, 941–942
- threat modeling
 - attack trees, 386–387
 - Cyber Kill Chain, 387–389
 - importance, 389–390
 - MITRE ATT&CK framework, 389
 - network security, 598
 - overview, 385
 - site and facility security, 418–419
 - software development design, 1086
 - STRIDE, 387–388
 - third-party connectivity, 705
- threat trees in software development design, 1086
- threat working group (TWG), 92

- threats
 - cybercriminals, 60
 - defined, 8
 - duress, 931–932
 - hacktivists, 61
 - identifying, 62–63
 - internal actors, 61–62
 - nation-state actors, 60–61
 - nature, 62
 - overview, 58
 - site planning, 423
- three-factor authentication, 719
- three-way-handshake process
 - SIP, 689
 - TCP, 949–951
- throughput in cabling, 654–655
- thunking, 296
- ticket granting services (TGSs) in KDC, 785–786
- tickets in KDC, 785–788
- Tier 1 (organization view) in risk management, 55
- Tier 2 (mission/business process view) in risk management, 55
- tiers
 - Cybersecurity Framework, 182
 - risk management, 55
- tight coupling software, 1131–1132
- time division multiple access (TDMA)
 - GTS, 570
 - mobile communications, 584
- time-division multiplexing (TDM), 541–542
- time-limited trials for third-party software, 1147
- time-of-check to time-of-use (TOC/TOU)
 - in atomic execution, 410
- time to first byte (TTFB) in latency, 654
- Time to Live (TTL) values in packets, 512
- TIME-WAIT state in TCP connections, 951
- timely characteristic in threat intelligence, 941
- timeouts in session termination, 741
- timing attacks in cryptography, 371–372
- timing smart cards, 735
- TKIP (Temporal Key Integrity Protocol), 577–578
- TLS. *See* Transport Layer Security (TLS)
- TOC/TOU (time-of-check to time-of-use)
 - in atomic execution, 410
- TOGAF (The Open Group Architecture Framework), 172, 194–195
- token passing, 491–492
- Token Ring, 495–496, 499
- tokens
 - electronic access control, 925
 - one-time passwords, 730
- toll fraud
 - IP telephony, 692
 - PBX systems, 666
- tool sets for secure software, 1138
- top-down approach in security programs, 199
- top-level domains in DNS, 527
- top secret classification level, 216–218
- topologies for local area networks, 487–490
- Tor network, 665
- TOR (The Onion Router), 307
- tort law system, 127–129
- Total Access Communication System (TACS), 584
- total risk vs. residual risk, 81
- TPC (Transmit Power Control), 574
- TPMs (Trusted Platform Modules), 404–406
- TPs (transformation procedures)
 - in Clark-Wilson model, 400
- Traceroute tool, 520–522
- tracking
 - digital asset management, 261–262
 - hardware, 224
 - software, 224–227
- trade secrets, 148–149
- trademarks, 150
- traffic direction in packet-filtering firewalls, 948
- traffic-flow security, 601
- traffic shaping in QoS, 551
- trailer hot sites, 1049
- training, 40
 - artificial intelligence tools, 977–978
 - content reviews, 43
 - degrees and certifications, 40–41
 - disaster recovery communications, 1057
 - disaster recovery plans, 1060–1061, 1064–1065
 - evaluating, 43–44
 - incident response, 993
 - measuring security, 863–867
 - methods and techniques, 41–43
 - personnel, 930–931

- training mode in anomaly-based IDS/IPS, 967
 - transactions, synthetic, 832
 - transborder data flow (TDF), 146–147
 - transfer risk strategy
 - ISO/IEC 27005, 178
 - overview, 79
 - transfers in personnel security, 37–38
 - transformation procedures (TPs)
 - in Clark-Wilson model, 400
 - Transmission Control Protocol (TCP)
 - connection-oriented protocol, 479
 - data structures, 509
 - handshakes, 508, 949–951
 - transport layer, 479, 503
 - vs. UDP, 503–506
 - Transmission Control Protocol/Internet Protocol (TCP/IP) suite, 471, 502–503
 - transmission media
 - cabling, 648–655
 - overview, 643–644
 - types, 644–648
 - transmission methods for local area networks, 499–500
 - Transmit Power Control (TPC), 574
 - transparent bridging, 656–657
 - transponders, 925
 - transport adjacency in IPSec, 609
 - transport layer
 - functions and protocols, 484
 - OSI model, 479–480
 - Transport Layer Security (TLS)
 - data in motion, 255–256
 - malware using, 604–605
 - network security, 602–605
 - suites, 603–604
 - types, 610–611
 - transport supplies in forensics field kits, 1015
 - transposition ciphers, 318
 - travel safety, 930
 - tree topology, 488
 - trials for third-party software, 1147
 - trialware, 153
 - TrickBot Trojan, 604, 969
 - Trojans in TLS, 604
 - trust but verify principle
 - network security, 599
 - secure architectures, 392
 - site and facility security, 420
 - third-party connectivity, 706
 - web services, 612
 - Trust Centers for mobile communications, 572
 - trust in federated identity, 755
 - Trusted Computing Group (TCG), 404
 - trusted execution environments (TEEs), 408–411
 - Trusted Platform Modules (TPMs), 404–406
 - TTFB (time to first byte) in latency, 654
 - TTL (Time to Live) values in packets, 512
 - TTXs (tabletop exercises) in disaster recovery plans, 1063–1064
 - tumbler locks, 918
 - tuning data loss prevention, 270–271
 - tunnels
 - DNS, 619
 - ICMP, 520
 - IPv6, 514–515
 - TLS, 610
 - turnstiles, 441
 - Tuzman, Kaleil Isaza, 20
 - TWG (threat working group), 92
 - twisted-pair cabling, 649–650
 - two-factor authentication (2FA), 719
 - type 1 hypervisors in virtual machines, 297
 - type 2 hypervisors in virtual machines, 297
 - Type I errors in biometric authentication, 724–725
 - Type II errors in biometric authentication, 724–725
 - types in incidents classification, 1002
- ## U
- U.S. Patent and Trademark Office (USPTO), 150
 - UAC (User Agent Client) in SIP, 689
 - UAS (User Agent Server) in SIP, 689
 - ubiquitous computing, 305
 - UBR (unspecified bit rate) in ATM, 551
 - UC (unified communications), 695–696
 - UCDs (use case diagrams) in software development, 1083
 - UDIs (unconstrained data items) in Clark-Wilson model, 400
 - UDP. *See* User Datagram Protocol (UDP)
 - UEBA (user and entity behavior analytics), 981

- UEM (unified endpoint management) systems, 226
 - UML (Unified Modeling Language)
 - software development, 1083
 - use case diagrams, 835–836
 - uncertainty in risk assessment, 74
 - unclassified classification level, 216–218
 - unconstrained data items (UDIs)
 - in Clark-Wilson model, 400
 - undercover investigations in digital forensics, 1020
 - understanding factor in outsourced security services, 974
 - unicast transmission method, 499
 - unified communications (UC), 695–696
 - unified endpoint management (UEM) systems, 226
 - Unified Modeling Language (UML)
 - software development, 1083
 - use case diagrams, 835–836
 - uniform resource identifiers (URIs) for web services, 613–614
 - uniform resource locators (URLs) in DNS, 524, 531
 - uninterruptible power supplies (UPSs)
 - data processing facilities, 446
 - online, 452–453
 - standby, 453
 - unit testing in software development, 1089, 1091
 - United States laws for data breaches, 141–142
 - unmanaged patching, 904–905
 - unshielded twisted pair (UTP) cable, 649–650
 - unspecified bit rate (UBR) in ATM, 551
 - updates
 - Internet of Things, 307
 - profiles, 740
 - UPS Brown color, 150
 - UPSs (uninterruptible power supplies)
 - data processing facilities, 446
 - online, 452–453
 - standby, 453
 - upstream suppliers in risk management, 98
 - uptime in high availability, 1050
 - urgency in incidents classification, 1002
 - URIs (uniform resource identifiers) for web services, 613–614
 - URLs (uniform resource locators) in DNS, 524, 531
 - usage in TCP vs. UDP, 506
 - use case diagrams (UCDs) in software development, 1083
 - use cases
 - data loss prevention, 271
 - misuse case testing, 835–836
 - Use Limitation Principle in OECD, 142
 - user access review for identity and access, 797
 - user-activated readers, 925
 - User Agent Client (UAC) in SIP, 689
 - User Agent Server (UAS) in SIP, 689
 - user and entity behavior analytics (UEBA), 981
 - user data file backups, 861
 - User Datagram Protocol (UDP)
 - connectionless protocol, 479
 - connections, 951–952
 - vs. TCP, 503–506
 - transport layer, 479
 - user-level event audits, 743
 - user managers, 24
 - user stories in Agile methodologies, 1101
 - users
 - Clark-Wilson model, 400
 - description, 25
 - provisioning, 739
 - USPTO (U.S. Patent and Trademark Office), 150
 - utilities
 - electric power, 448–453
 - HVAC, 453–454
 - water and wastewater, 448–450
 - utility tunnels in physical security, 439
 - UTP (unshielded twisted pair) cable, 649–650
- ## V
- vacations, mandatory, 35, 890
 - Valasek, Chris, 627
 - validation
 - assessments, 815–816
 - parameters, 1132
 - risk controls, 90
 - software development, 1090
 - Validation practice in Good Practice Guidelines, 106
 - valuation of assets, 65–66
 - variable bit rate (VBR) in ATM, 551
 - vaulting for backups, 1038–1039
 - vaults, protecting, 222

- VBR (variable bit rate) in ATM, 551
- VDI (virtual desktop infrastructure), 700–701
- VDSL (very high-data-rate DSL), 684
- vendors, 39
- ventilation ducts in physical security, 439
- Veracode report, 1133
- verifiable property for reference monitors, 766
- verification
 - backups, 860–862
 - message integrity, 354–358
 - risk controls, 90
 - software development, 1090
 - supply chain risk management, 100
- verification 1:1, 718
- Verification function in SAMM, 1109
- Vernam, Gilbert, 325
- Vernam cipher, 325–328
- versatile memory in Trusted Platform Modules, 406
- versioning software, 1142–1144
- vertical enactment for privacy, 147
- very high-data-rate DSL (VDSL), 684
- very high-level programming languages, 1119–1120
- very small aperture terminals (VSATs), 589–590
- vibration detectors, 927
- VIDs (VLAN identifiers), 631
- views in enterprise architecture frameworks, 190, 192
- Vigenère, Blaise de, 319
- Vigenère cipher, 319
- violence, threats of, 931–932
- virtual circuits in WANs, 548–549
- virtual desktop infrastructure (VDI), 700–701
- virtual directories, 750
- Virtual eXtensible Local Area Networks (VxLANs), 632
- virtual firewalls, 964
- virtual local area networks (VLANs)
 - latency, 654
 - overview, 630–632
- virtual machines (VMs), 296, 704–705
 - antimalware, 969–970
 - benefits, 297–298
 - hypervisors, 297
 - third-party connectivity, 705
- Virtual Network Computing (VNC), 700
- virtual NICs (vNICs), 704–705
- virtual passwords, 723
- virtual private clouds (VPCs), 301
- virtual private networks (VPNs)
 - authentication protocols, 697–699
 - data in motion, 256
 - IPSec, 607–609
 - L2TP, 606–607
 - overview, 605, 697
 - PPTP, 606
 - TLS, 610
- Virtual Router Redundancy Protocol (VRRP), 536
- virtual teams in incident response, 991
- virtual tunnel end points (VTEPs), 632
- virtualization
 - backups, 861
 - desktop, 699–701
- virtualized systems
 - containerization, 298–299
 - networks, 704–705
 - overview, 296
 - serverless, 299–301
 - virtual machines, 296–298
- visual recording devices, 913–916
- VLAN identifiers (VIDs), 631
- VLANs (virtual local area networks)
 - latency, 654
 - overview, 630–632
- VMs. *See* virtual machines (VMs)
- VNC (Virtual Network Computing), 700
- vNICs (virtual NICs), 704–705
- voice communications, 682
 - cable modems, 686–687
 - DSL, 683–685
 - IP telephony, 687–692
 - ISDN, 685–686
 - PSTN, 682–683
- voice gateways, 688
- voice over IP (VoIP) networks
 - business continuity planning, 1069
 - vs. IP telephony, 688
 - overview, 687–688
 - security, 693
- voice prints, 728
- voicemail systems, 688
- voices in information access control, 801

- voltage in electrical power, 670
- voltage regulators for electric power, 451
- volumetric IDSs, 926
- VPCs (virtual private clouds), 301
- VPNs. *See* virtual private networks (VPNs)
- VRRP (Virtual Router Redundancy Protocol), 536
- VSATs (very small aperture terminals), 589–590
- VTEPs (virtual tunnel end points), 632
- vulnerabilities
 - defined, 8
 - emergency situations, 869
 - exception handling, 871
 - human, 902–903
 - identifying, 62–63
 - information, 59
 - managing, 900–903
 - overview, 58
 - people, 60
 - processes, 59–60, 902
 - remediation, 871
 - software, 901, 1133–1134
 - testing, 817–822
- vulnerability mapping step in penetration testing, 824
- vulnerability testing vs. penetration tests, 827
- VxLANs (Virtual eXtensible Local Area Networks), 632

W

- wafer tumbler locks, 919
- waiting room feature for meeting applications, 694
- walkthrough tests in disaster recovery plans, 1063
- walls
 - considerations, 437
 - data processing facilities, 446
- WANs. *See* wide area networks (WANs)
- WAPs (wireless access points), 564–565
- warded locks, 918
- warez sites, 149–150
- warm sites, 1045–1047
- Wassenaar Arrangement, 145–146
- water and wastewater, 448–450
- water detectors, 445
- water lines, 438
- water sprinklers, 459–460
- Waterfall software development, 1095–1096
- watts
 - electrical power, 670–672
 - radio signals, 560
- wave-division multiplexing (WDM), 544
- wave-pattern motion detectors, 927
- WBSs (work breakdown structures) in project management, 1081
- WDM (wave-division multiplexing), 544
- weaponization in Cyber Kill Chain model, 387, 994
- web application security risks, 1134
- web of trust, 367
- web portal functions in FIM systems, 753–754
- web proxies, 665
- web services
 - HTTP, 613–614
 - overview, 611–612
 - REST, 615–616
 - SOAP, 614–615
- Web Services Security (WS-Security or WSS) specification, 615
- well-formed transactions in Clark-Wilson model, 400
- well-known ports, 507
- WEP (Wired Equivalent Privacy), 575–576
- wet chemical fire extinguishers, 459
- wet pipe water sprinkler systems, 460
- whaling, 865
- White, Joe, 20
- white box testing, 826
- whitelisting
 - applications, 225
 - intrusion detection and prevention systems, 968–969
- whole-disk encryption, 255
- Wi-Fi Protected Access 2 (WPA2), 576–578
- wide-angle lenses in CCTV systems, 915
- wide area networks (WANs)
 - ATM, 550–552
 - CSU/DSU, 543–545
 - dedicated links, 541–543
 - frame relay, 547–548
 - HSSI, 552
 - overview, 540
 - switching, 545–547
 - virtual circuits, 548–549
 - X.25, 549–550

- WIDSs (wireless intrusion detection systems), 967
 - WiMAX standard, 569, 587
 - windows
 - considerations, 437
 - types, 441
 - WIPO (World Intellectual Property Organization), 150
 - Wired Equivalent Privacy (WEP), 575–576
 - wired windows, 441
 - wireless access points (WAPs), 564–565
 - wireless intrusion detection systems (WIDSs), 967
 - wireless LANs (WLANs)
 - best practices, 582
 - components, 564–565
 - security, 575–582
 - standards, 565–574
 - wireless networking
 - chapter questions, 592–595
 - chapter review, 590–592
 - communication techniques overview, 559–561
 - mobile communications, 582–588
 - OFDM, 563–564
 - overview, 559
 - satellites, 589–590
 - spread spectrum, 561–563
 - WLAN components, 564–565
 - WLAN security, 575–582
 - WLAN standards, 565–574
 - wireless personal area networks (WPANs), 570
 - wiring closets, 446
 - WLANs. *See* wireless LANs (WLANs)
 - Woods, John F., 1079
 - work area security, 441–443
 - work area separation, 803
 - work breakdown structures (WBSs)
 - in project management, 1081
 - work factor
 - cryptosystems, 325
 - electrical power, 671
 - work factor in RSA, 342
 - work recovery time (WRT) in disaster recovery, 1031–1032
 - working images for evidence, 1012
 - World Intellectual Property Organization (WIPO), 150
 - World Wide Web (WWW), 777
 - WPA Enterprise, 577
 - WPA2 (Wi-Fi Protected Access 2), 576–578
 - WPA3, 578–579
 - WPANs (wireless personal area networks), 570
 - write-once media for logs, 745, 831
 - wrongs against a person category
 - in civil law, 127
 - wrongs against property category
 - in civil law, 127
 - WRT (work recovery time) in disaster recovery, 1031–1032
 - WS-Security specification, 615
 - WSS (Web Services Security) specification, 615
 - WWW (World Wide Web), 777
- ## X
- X.25 protocol, 549–550, 552
 - X.509 certificates, 359
 - XaaS (Everything as a Service), 304–305
 - XACML (Extensible Access Control Markup Language), 781
 - XDR (extended detection and response)
 - platforms, 968
 - XML (Extensible Markup Language), 615, 777
 - XOR operation
 - one-time pads, 326–327
 - stream ciphers, 333
 - XTACACS (Extended TACACS), 790–791
 - YAML Ain't Markup Language (YAML), 615
- ## Y
- Ying, Jun, 20
- ## Z
- Zachman, John, 172, 192
 - Zachman Framework, 172, 192–194
 - zero-day attacks, 971
 - zero knowledge in penetration testing, 825
 - zero trust principle
 - network security, 599
 - secure design, 392
 - site and facility security, 419–420
 - third-party connectivity, 706
 - web services, 612
 - ZigBee standard, 571–572
 - Zimmermann, Phil, 367
 - zombies, 965

zone transfers in DNS, 525

zones

access control, 803

CPTED, 429–430

DNS, 525

lighting, 911

Zoom-bombing, 694

zoom in CCTV systems, 914–915