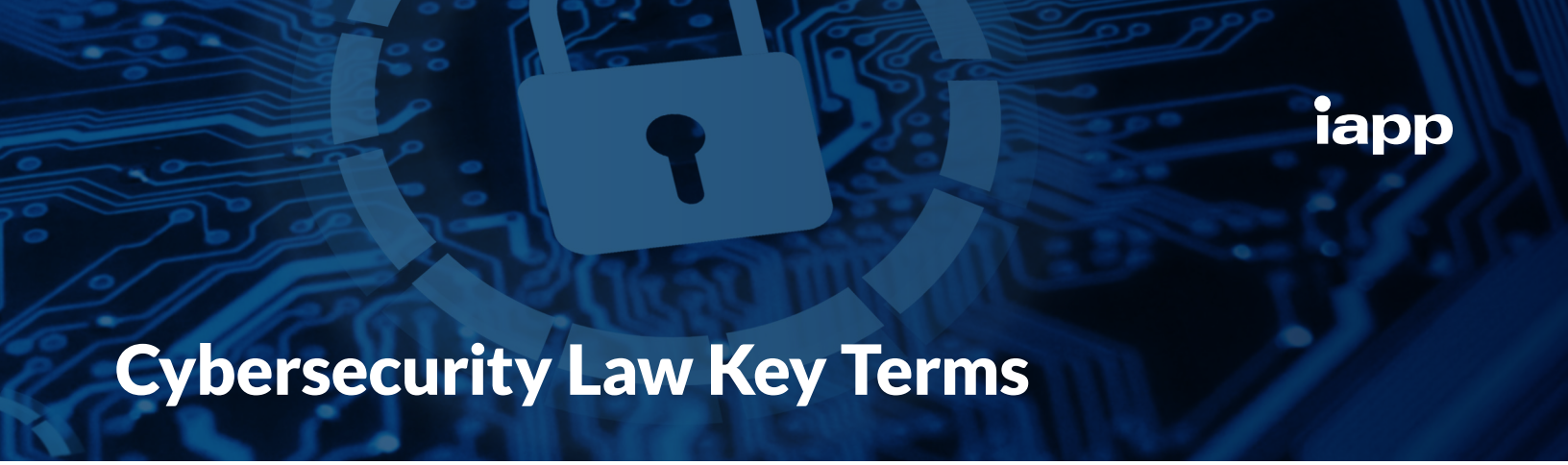

# Cybersecurity Law Key Terms

Cybersecurity law is like a patchwork quilt, stitched together with pieces from disparate doctrinal fields. It addresses not only data protection but also critical infrastructure and national security. Cyber resiliency now implicates many aspects of corporate and governmental operations, engaging senior management, boards of directors and policymakers at all levels. Understanding this rapidly developing field, like any other, requires a shared language. Hence, IAPP staff developed these key terms with valuable input from top experts in cybersecurity law.

Two notes on methodology. First, unlike other IAPP glossaries, this one does not aim to synthesize terminology across different laws and doctrinal fields. Instead, it quotes from or relies heavily on official definitions in statutes and government publications with links to specific sources so users can see the context and conduct their own further research. In a few cases, we amended the official definition, indicating new text with brackets. We did this where the statutory or other official definitions focused on information systems, but they could apply also to computer systems more broadly, such as operational technology. This reflects the relatively recent expansion of cybersecurity concerns from the protection of information to the protection of critical infrastructure and other operational technology controlling functions and services in the physical environment.

Second, these key terms are limited in this initial version to U.S. law at the federal and state level. Cybersecurity is a major concern in almost every country, and many nations and regions are developing complex and sophisticated bodies of law for cybersecurity. As an initial step, it is impossible to develop a single common resource covering all these efforts. The IAPP will strive to internationalize these key terms in the future.

This resource was originally published in January 2026. It will be updated regularly and as needed to reflect the developing state of cybersecurity law.

Although there are some shared terms and definitions, these key terms are separate from the official IAPP Glossary of Privacy Terms. See also the IAPP's Key Terms for AI Governance.

| TERM | DEFINITION |
|---|---|
| **Access** | Under the Computer Fraud and Abuse Act, the act of entering a computer system or a particular part of a computer system, such as files, folders or databases.<br>**Source:** Van Buren v. United States, 593 U.S. 374, 388, 141 S. Ct. 1648, 1657 (2021) |
| **Access control** | The process of granting or denying specific requests for or attempts to obtain and use information and related information processing services, enter specific physical facilities, or access a specific computer system or device.<br>**Sources:** Glossary, National Initiative for Cybersecurity Careers and Studies; Glossary, NIST Computer Security Resource Center |
| **Advanced persistent threat** | A cyber adversary, such as a nation-state or a ransomware network, that possesses sophisticated levels of expertise and significant resources that allow it, by using multiple attack vectors like vulnerability exploitation, credential abuse, and social engineering, to create opportunities within a computer network to achieve its objectives. These objectives typically include establishing and extending footholds within the technology infrastructure of the targeted organization for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization or positioning itself to carry out these objectives in the future. The advanced persistent threat pursues its objectives repeatedly over an extended period of time and adapts to defenders' efforts to resist it.<br>**Sources:** NIST SP 800-39; Glossary, NICCS; Glossary, CSRC; Project Upskill Glossary \| Cybersecurity and Infrastructure Security Agency |
| **Authentication** | The process of verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a computer system.<br>**Source:** Glossary, CSRC |
| **Backup** | A copy of files and programs made to facilitate recovery if necessary.<br>**Source:** Glossary, CSRC |
| **Breach** | The unauthorized access to or acquisition of computerized data that compromises the security, confidentiality or integrity of personal information. Note: Definitions of "personal information" vary across different laws, regulations and enforcement regimes. Breach may refer more generally to the compromise of the security of a computer system or network. See also "data breach" and "cyber incident."<br>**Sources:** Cal. Civ. Code 1.81 § 1798.82; New York Gen. Bus. Law, 39-F § 899-AA. See also Glossary, CSRC. |
| **Breach notification** | The legal requirement, under law or contract, to inform individuals, third parties, and/or governmental authorities that personal information has been compromised. See also "incident reporting/disclosure."<br>**Source:** Cybersecurity Law Fundamentals, 2nd ed. pp. 63-64 |

| TERM | DEFINITION |
|---|---|
| **Cloud computing** | "A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."<br>**Source:** Glossary, CSRC |
| **Computer crime** | Offenses directed at computers or computerized data, such as unauthorized access to or deletion of data or rendering data or computing resources unavailable. See also "cybercrime."<br>**Source:** Cybersecurity Law Fundamentals, 2nd ed. pg.16 |
| **Computer security** | Measures and controls intended to ensure confidentiality, integrity, and availability of computer systems or the information processed and stored by a computer.<br>**Source:** Glossary, CSRC citing Committee on National Security Systems Instruction 4009-2015 |
| **Computer trespass** | Under the CFAA, intentionally and without authorization accessing any nonpublic computer.<br>**Source:** 18 U.S.C. § 1030(a)(3) |
| **Confidentiality** | "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information."<br>**Sources:** Glossary, CSRC; Glossary, NICCS; 44 USC § 3552(a)(3)(B) |
| **Controls** | The safeguards or countermeasures prescribed for an information or computer system or an organization to protect the confidentiality, integrity, and availability of the system and its information. Cybersecurity controls include policies, procedures, guidelines, practices, or organizational structures, which can be of an administrative, technical, management or legal nature.<br>**Sources:** NIST SP 800-37 Rev. 2; Information Systems Audit and Control Association Glossary of Terms |
| **Critical infrastructure** | "Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."<br>**Source:** 42 U.S.C. § 5195c(e) |
| **Cybercrime** | "Offenses directed at computers or computerized data: trespass into a computer system or data base; theft of credit card information, trade secrets, or other data stored in a computer system; alteration or destruction of such data; interference with access to data or online services; or extortion by hijacking or threatening to damage a computer system or data." See also "computer crime."<br>**Source:** Cybersecurity Law Fundamentals, 2nd ed. pg.16 |

| TERM | DEFINITION |
|---|---|
| **Cyber incident** | "An occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information [or computer] system, or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies." See also "cybersecurity event."<br>**Source:** 44 U.S.C. § 3552(2). Compare, however, 6 U.S.C. § 650(12) and 6 U.S.C. § 681(5), the latter of which excludes an occurrence that imminently, but not actually, jeopardizes (i) information on information systems; or (ii) information systems. See also FIPS Publication 200. |
| **Cyber operations** | In military parlance, the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace, where a "cyberspace capability" is defined as "a device or computer program, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace."<br>**Source:** CNSSI 4009-2015 from DoD JP 3-12 |
| **Cybersecurity event** | "Any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an information system or information stored on such information system." See also cyber incident.<br>**Source:** New York State Department of Financial Services Cybersecurity Requirements, 23 NYCRR 500 |
| **Cybersecurity risk** | "Threats to and vulnerabilities of information or information [or computer] systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of such information or information [or computer] systems, including such related consequences caused by an act of terrorism. Does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement."<br>**Source:** 6 U.S.C. § 650(7) |
| **Cybersecurity service providers** | Third-party organizations that offer a range of services to help entities protect their data, systems, and networks from cybersecurity threats. Also known as managed security service providers, their services may include monitoring, virtual private networks, managed firewalls, and antivirus management as well as cybersecurity incident remediation and investigation. Managed service providers provide a wider range of outsourced management of an entity's devices and systems, which may include security services.<br>**Source:** IBM. See also 6 U.S.C. § 650(18). |
| **Cybersecurity threat** | Anything that has the potential to cause serious harm to a computer system. Specifically, "an action, not protected by the First Amendment to the Constitution of the United States, on or through an information [or computer] system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information [or computer] system or information that is stored on, processed by, or transiting an information system," but not including "any action that solely involves a violation of a consumer term of service or a consumer licensing agreement."<br>**Sources:** 6 U.S.C. § 650(8); Glossary, NICCS |

| TERM | DEFINITION |
|---|---|
| **Cyber threat indicator** | "Information that is necessary to describe or identify— (A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability; (B) a method of defeating a security control or exploitation of a security vulnerability; (C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability; (D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability; (E) malicious cyber command and control; (F) the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat; (G) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or (H) any combination thereof."<br>**Source:** 6 U.S.C. § 650(5) |
| **Damaging computers** | Under the CFAA, "any impairment to the integrity or availability of data, a program, a system, or information."<br>**Source:** 10 U.S.C. § 1030(e)(8) |
| **Data breach** | The "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person or business." Depending on applicable law, a data breach may trigger notification requirements, subject to a safe harbor for encrypted information and, under some state laws, a harm analysis. See also "breach" and "cyber incident."<br>**Source:** Cal. Civil Code § 1798.82(g). See also 45 C.F.R. § 164.402 (Health Insurance Portability and Accountability Act breach notice rule); 16 C.F.R. § 314.2(m) (FTC Gramm-Leach-Bliley Act safeguards rule); NICCS; CISA Glossary. |
| **Data minimization** | Principle that organizations should only "create, collect, use, process, store, maintain, disseminate or disclose [personally identifiable information] that is directly relevant and necessary to accomplish a legally authorized purpose, and should only maintain PII for as long as is necessary to accomplish the purpose."<br>**Source:** Fair Information Practice Principles (FIPPs) \| FPC.gov. See also Cal. Civil Code § 1798.100(c); Cal. Code Regs. tit. 11 § 7002(d). |

| TERM | DEFINITION |
|---|---|
| **Data protection** | The legal requirement or the administrative, technical and physical strategies and processes for "safeguarding important data from corruption, compromise or loss and providing the capability to restore the data to a functional state should something happen to render the data inaccessible or unusable."<br>**Source:** Storage Networking Industry Association<br>**Data protection** also refers to "the rules and safeguards applying under various laws and regulations to personal data about individuals that organizations collect, store, use and disclose. 'Data protection' is the professional term used in the EU, whereas in the U.S. the concept is generally referred to as 'information privacy.'" When used in this context, "data protection is different from data security, since it extends beyond securing information to devising and implementing policies for its fair use."<br>**Source:** IAPP Glossary of Privacy Terms |
| **Decryption key** | A piece of information, often a string of numbers or letters, which, when processed through a cryptographic algorithm, can decode encrypted data.<br>**Sources:** See "key" and "decryption key" in Glossary, CSRC. |
| **Defensive measure** | "An action, device, procedure, signature, technique, or other measure applied to an information [or computer] system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability."<br>**Source:** 6 U.S.C. § 650(9)(A) |
| **Denial-of-service ("DoS") attack** | A cyberattack where "legitimate users are unable to access information systems, devices, or other network resources," e.g., email, websites, or online accounts, "due to the actions of a malicious cyber threat actor." "Accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users."<br>**Source:** CISA, "Understanding Denial-of-Service Attacks" |
| **Duty** | One element of a negligence claim under the common law. In data breach and other cybersecurity incident litigation, a threshold question on any claim of negligence is whether the defendant had a duty to protect the data or network, provide notice of incidents, or take other preventative or responsive actions.<br>**Source:** Cybersecurity Law Fundamentals, 2nd ed. pgs.136-38 |
| **Encryption** | "The process of transforming plaintext into ciphertext using a cryptographic algorithm and key," thereby concealing the data's meaning to prevent it from being known or used.<br>**Source:** NIST SP 800-56B Rev. 2 |
| **Exceeds authorized access** | Under CFAA, "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."<br>**Source:** 18 U.S.C. § 1030(e)(6). See also Van Buren v. United States, 593 U.S. 381-88, 141 S. Ct. 1648, 1657-58 (2021). |

| TERM | DEFINITION |
|---|---|
| **Extortion** | In the cybersecurity context, to extort or attempt to extort from any person any money or other thing of value by transmitting "any communication containing any (A) threat to cause damage to a protected computer; (B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or (C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion."<br>**Source:** 18 U.S.C. § 1030(a)(7) |
| **Forensic analysis** | "The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data." In the cybersecurity context, generally performed after a cybersecurity incident to determine the cause and scope of, and actors involved in, the incident.<br>**Source:** 32 C.F.R. § 236.2 |
| **Hostile acts exclusion** | A clause in insurance policies excluding coverage for losses due to hostile or warlike acts, often invoked by carriers when claims arise from a state-sponsored cyber incident.<br>**Source:** Cybersecurity Law Fundamentals, 2nd ed. pgs. 129-30 |
| **Identity management** | The methods and processes used to manage subjects (such as individual users) and their authentication and authorizations (privileges) to access specific objects (such as devices, networks or information). Sometimes referred to as identity and access management.<br>**Source:** Glossary, NICCS |
| **Identity theft** | "All types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain."<br>**Source:** U.S. Department of Justice: Identity Theft. See also 18 U.S.C. § 1028. |
| **Incident response** | Coordinated activities and procedures to detect, analyze, contain, remediate, and recover from cyber incidents, in order to minimize harm, comply with legal requirements and maintain or promptly restore operations.<br>**Source:** NIST SP 800-61 Rev. 2 |
| **Information operations** | The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.<br>**Source:** Department of Defense JP 3-13 |
| **Information security** | The protection, through administrative, technical and physical safeguards, of "information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide" integrity, confidentiality and availability.<br>**Source:** 44 U.S.C. § 3552(a)(3) |

| TERM | DEFINITION |
|---|---|
| **Information technology** | Any equipment or interconnected system or subsystem of equipment that processes, transmits, receives, or interchanges data or information.<br><br>"[A]ny equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information ... . includes computers, ancillary equipment ..., peripheral equipment ..., software, firmware and similar procedures, services (including support services), and related resources."<br><br>**Sources:** NIST SP 800-53 rev. 5; 40 U.S.C. § 11101(6). |
| **Intrusion detection** | "The process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices."<br><br>**Source:** NIST SP 800-94 |
| **Malware** | Software or firmware intended or designed or to perform an unauthorized process that will have adverse impacts on the confidentiality, integrity or availability of an information or computer system.<br><br>**Source:** NIST SP 800-53 rev. 5 |
| **Monitoring** | Continuously observing and analyzing a network, its traffic, the devices on the network and the data stored on the network to identify modifications or behavioral anomalies indicative of security threats, vulnerabilities, compromises or policy violations<br><br>**Source:** CISA |
| **Multifactor authentication** | Authentication method using two or more factors to achieve authentication. Factors include: something you know, e.g., password or personal identification number; something you have, e.g., cryptographic identification device, token, ATM card, smartphone; or something you are, e.g., biometric.<br><br>**Sources:** NIST SP 1800-17b; NIST SP 800-171r3 |
| **Operational technology** | "A broad range of programmable systems and devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems and devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events." Examples include industrial control systems, building management systems, fire control systems and physical access control mechanisms.<br><br>**Source:** NIST SP 800-82r3 |
| **PCI DSS** | The Payment Card Industry Data Security Standard is an information security standard administered by the Payment Card Industry Security Standards Council for merchants, banks and other entities that process payments involving branded credit cards from the major card schemes.<br><br>**Source:** NIST SP 1800-16B. See also PCI Security Standards Council. |

| TERM | DEFINITION |
|---|---|
| **Personal information** | Varies from state to state and law to law.<br><br>Under the California Consumer Privacy Act, "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."<br><br>**Source:** Cal. Civil Code tit. 1.81.5 § 1798.140(v)(1)<br><br>A similar definition is used by many of the state "comprehensive" privacy laws.<br><br>However, state data breach notification laws often have a narrower definition. Under California's breach notification law, "personal information" means either of the following:<br><br>"(1) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:<br><br>(A) Social security number.<br><br>(B) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.<br><br>(C) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.<br><br>(D) Medical information.<br><br>(E) Health insurance information.<br><br>(F) Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.<br><br>(G) Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.<br><br>(H) Genetic data.<br><br>(2) A username or email address, in combination with a password or security question and answer that would permit access to an online account."<br><br>**Source:** Cal. Civil Code tit. 1.81 § 1798.82(h) |
| **Personally identifiable information** | "Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."<br><br>**Source:** Office of Management and Budget Circular No. A-130 |
| **Phishing** | "A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a Web site, in which the perpetrator masquerades as a legitimate business or reputable person."<br><br>**Source:** Internet Engineering Task Force RFC 4949 Ver 2. See also the latest annual report of the Anti-Phishing Working Group. |

| TERM | DEFINITION |
|---|---|
| **Privacy impact assessment** | As required within the federal government under the E-Government Act, "an analysis of how information is handled to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; to determine the risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of information in identifiable form in an electronic information system; and to examine and evaluate protections and alternate processes for handling information to mitigate potential privacy concerns. A privacy impact assessment is both an analysis and a formal document detailing the process and the outcome of the analysis."<br>**Source:** OMB Circular A-130 (2016). See also IAPP Glossary of Privacy Terms.<br>**Related terms:** Many comprehensive state privacy laws require a "data protection assessment." California law requires an annual cybersecurity audit. Article 35 of the EU General Data Protection Regulation requires controllers to undertake a "data protection impact assessment" of any processing likely to result in a high risk to the rights and freedoms of natural persons. |
| **Proprietary information** | "Material and information relating to or associated with a company's products, business, or activities, including but not limited to financial information; data or statements; trade secrets; product research and development; existing and future product designs and performance specifications; marketing plans or techniques; schematics; client lists; computer programs; processes; and know-how that has been clearly identified and properly marked by the company as proprietary information, trade secrets, or company confidential information. The information must have been developed by the company and not be available to the government or to the public without restriction from another source."<br>**Source:** Glossary, CSRC |
| **Protected computer** | Under the CFAA, a computer<br>"(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government;<br>(B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States; or<br>(C) that-<br>(i) is part of a voting system; and<br>(ii)(I) is used for the management, support, or administration of a Federal election; or<br>(II) has moved in or otherwise affects interstate or foreign commerce."<br>**Source:** 18 U.S.C. § 1030(e)(2) |

| TERM | DEFINITION |
|---|---|
| **Protected health information** | For purposes of HIPAA, "individually identifiable health information:<br>(1) Except as provided in paragraph (2) of this definition, that is:<br>(i) Transmitted by electronic media;<br>(ii) Maintained in electronic media; or<br>(iii) Transmitted or maintained in any other form or medium.<br>(2) Protected health information excludes individually identifiable health information:<br>(i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;<br>(ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv);<br>(iii) In employment records held by a covered entity in its role as employer; and<br>(iv) Regarding a person who has been deceased for more than 50 years."<br>**Source:** 45 C.F.R. § 160.103<br>In HIPAA itself, health information is defined as "any information, whether oral or recorded in any form or medium, that— (A) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual."<br>**Source:** 42 U.S.C. § 1320d(4) |
| **Ransomware** | A form of malware that encrypts files on a device, rendering them unusable, with the malicious actors demanding ransom in exchange for decryption, often accompanied by a threat to sell or publicly release the data if the ransom is not paid, although some attackers skip the encryption step and demand ransom to not release stolen files.<br>**Source:** CISA |
| **Resilience** | "The ability to continue to (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs."<br>**Source:** NIST SP 800-137 from NIST SP 800-39 |
| **Risk assessment** | The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, and other organizations resulting from the operation of a system. Part of risk management, it incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place.<br>**Sources:** NIST SP 800-39; NIST SP 800-30 rev 1 |
| **Scraping** | Automated extracting of data from a website and copying it for manipulation, analysis or other reuse.<br>**Source:** hiQ Labs v. LinkedIn Corp., 31 F.4th 1180, 1186 n.4 (9th Cir. 2022) |

| TERM | DEFINITION |
|---|---|
| **Security audit** | "Independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures."<br>**Source:** NIST SP 800-82r3 from ISO/IEC 7498-1:1994 |
| **Supply chain attack** | An attack in which the adversary inserts a vulnerability into the product of an upstream provider, such as a software developer or software library, prior to its installation, allowing the adversary to compromise the systems of downstream users of that product.<br>**Source:** CNSSI 4009-2015 CISA |
| **Threat intelligence** | "Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes."<br>**Source:** NIST SP 800-150. See also: NIST SP 800-172; NIST SP 800-172A |
| **Trafficking (passwords)** | Under federal law, "to transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of," any password or similar information through which a computer may be accessed without authorization.<br>**Source:** 18 U.S.C. § 1029 |
| **Vulnerability** | A weakness in an information system, system security procedures, internal controls or implementation that could be exploited or triggered by a threat source.<br>**Source:** NIST SP 800-30 Rev. 1 |
| **Vulnerability disclosure** | The process in which third parties, including independent security researchers, discover vulnerabilities in products or systems and report those to the product developers or system operators and for those developers or operators to receive such vulnerability reports and take remedial action, such as issuing patches.<br>**Sources:** Cybersecurity Law Fundamentals, 2nd ed. pgs. 217, 481; NIST SP 800-216 |
| **Zero-day** | A previously unknown hardware, firmware, or software vulnerability, referred to as a zero-day vulnerability, or an attack exploiting such a vulnerability, referred to as a zero-day attack, in reference to the product developer having zero days to patch the flaw and defenders having zero days to prepare before it is exploited.<br>**Source:** IBM |

# Key terms






Updated December 2025.

Find the latest version at iapp.org/resources