

## **CYBERSECURITY TERMS**

This cybersecurity resource covers Security Principles, Incident Response, Business Continuity, Access Control, Network Security, and Security Operations, offering clear and concise explanations of key concepts like administrative controls, cryptographic methods, and risk management. It provides a straightforward guide to mastering essential cybersecurity terminology.

### **SECTION ONE: SECURITY PRINCIPLES**

1. Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse or unauthorized access to or modification of information.

#### Adequate Security

2. Controls implemented through policy and procedures. Examples include access control processes and requiring multiple personnel to conduct a specific operation.

Administrative controls in modern environments are often enforced in conjunction with physical and/or technical controls, such as an access-granting policy for new users that requires login and approval by the hiring manager.

#### Administrative Controls

3. The ability of computers and robots to simulate human intelligence and behavior.

#### Artificial Intelligence

4. Anything of value that is owned by an organization. Assets include both tangible items such as information systems and physical property and intangible assets such as intellectual property.

#### Asset

5. Access control process validating that the identity being claimed by a user or entity is known to the system, by comparing one (single factor or SFA) or more (multi-factor authentication or MFA) factors of identification.

#### Authentication

6. The right or a permission that is granted to a system entity to access a system resource.

#### Authorization

7. Ensuring timely and reliable access to and use of information by authorized users.

#### Availability

8. A documented, lowest level of security configuration allowed by a standard or organization.

#### Baseline

9. Biological characteristics of an individual, such as a fingerprint, hand geometry, voice, or iris patterns.

#### Biometric

10. Malicious code that acts like a remotely controlled "robot" for an attacker, with other Trojan and worm capabilities.

#### Bot

11. Information that has been determined to require protection against unauthorized disclosure and is marked to indicate its classified status and classification level when in documentary form.

#### Classified or Sensitive Information

12. The characteristic of data or information when it is not made available or disclosed to unauthorized persons or processes.

#### Confidentiality

13. A measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function.

#### Criticality

14. The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing and while in transit.

#### Data integrity

15. The process and act of converting the message from its plaintext to ciphertext. Sometimes it is also referred to as enciphering. The two terms are sometimes used interchangeably in literature and have similar meanings.

#### Encryption

16. In 2016, the European Union passed comprehensive legislation that addresses personal privacy, deeming it an individual human right.

#### General Data Protection Regulation (GDPR)

17. The process of how an organization is managed; usually includes all aspects of how decisions are made for that organization, such as policies, roles, and procedures the organization uses to make those decisions.

#### Governance

18. This U.S. federal law is the most important healthcare information regulation in the United States. It directs the adoption of national standards for electronic healthcare transactions while protecting the privacy of individual's health information. Other provisions address fraud reduction, protections for individuals with health insurance and a wide range of other healthcare-related activities.

#### Health Insurance Portability and Accountability Act (HIPAA)

19. The magnitude of harm that could be caused by a threat's exercise of a vulnerability.

#### Impact

20. The potential adverse impacts to an organization's operations (including its mission, functions and image and reputation), assets, individuals, other organizations, and even the nation, which results from the possibility of unauthorized access, use, disclosure, disruption, modification or destruction of information and/or information systems.

#### Information Security Risk

21. The property of information whereby it is recorded, used and maintained in a way that ensures its completeness, accuracy, internal consistency and usefulness for a stated purpose.

#### Integrity

22. The ISO develops voluntary international standards in collaboration with its partners in international standardization, the International Electro-technical Commission (IEC) and the International Telecommunication Union (ITU), particularly in the field of information and communication technologies.

#### International Organization of Standards (ISO)

23. The internet standards organization, made up of network designers, operators, vendors and researchers, that defines protocol standards (e.g., IP, TCP, DNS) through a process of collaboration and consensus.

#### Internet Engineering Task Force (IETF)

24. The probability that a potential vulnerability may be exercised within the construct of the associated threat environment.

#### Likelihood

25. A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or set of vulnerabilities.

## Likelihood of Occurrence

26. Using two or more distinct instances of the three factors of authentication (something you know, something you have, something you are) for identity verification.

## Multi-Factor Authentication

27. The NIST is part of the U.S. Department of Commerce and addresses the measurement infrastructure within science and technology efforts within the U.S. federal government. NIST sets standards in a number of areas, including information security within the Computer Security Resource Center of the Computer Security Divisions.

## National Institutes of Standards and Technology (NIST)

28. The inability to deny taking an action such as creating information, approving information and sending or receiving a message.

## Non-repudiation

29. The National Institute of Standards and Technology, known as NIST, in its Special Publication 800-122 defines PII as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial and employment information."

## Personally Identifiable Information (PII)

30. Controls implemented through a tangible mechanism. Examples include walls, fences, guards, locks, etc. In modern organizations, many physical control systems are linked to technical/logical systems, such as badge readers connected to door locks.

## Physical Controls

31. The right of an individual to control the distribution of information about themselves.

## Privacy

32. The chances, or likelihood, that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities.

#### Probability

33. Information regarding health status, the provision of healthcare or payment for healthcare as defined in HIPAA (Health Insurance Portability and Accountability Act).

#### Protected Health Information (PHI)

34. A method for risk analysis that is based on the assignment of a descriptor such as low, medium or high.

#### Qualitative Risk Analysis

35. A method for risk analysis where numerical values are assigned to both impact and likelihood based on statistical probabilities and monetarized valuation of loss or gain.

#### Quantitative Risk Analysis

36. A possible event which can have a negative impact upon the organization.

#### Risk

37. Determining that the potential benefits of a business function outweigh the possible risk impact/likelihood and performing that business function with no other action.

#### Risk Acceptance

38. The process of identifying and analyzing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals and other organizations. The analysis performed as part of risk management which incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place.

#### Risk Assessment

39. Determining that the impact and/or likelihood of a specific risk is too great to be offset by the potential benefits and not performing a certain business function because of that determination.

#### Risk Avoidance

40. The process of identifying, evaluating and controlling threats, including all the phases of risk context (or frame), risk assessment, risk treatment and risk monitoring.

#### Risk Management

41. A structured approach used to oversee and manage risk for an enterprise.

#### Risk Management Framework

42. Putting security controls in place to reduce the possible impact and/or likelihood of a specific risk.

#### Risk Mitigation

43. The level of risk an entity is willing to assume in order to achieve a potential desired result. Source: NIST SP 800-32. Risk threshold, risk appetite and acceptable risk are also terms used synonymously with risk tolerance.

#### Risk Tolerance

44. Paying an external party to accept the financial impact of a given risk.

#### Risk Transference

45. The determination of the best way to address an identified risk.

#### Risk Treatment

46. The management, operational and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity and availability of the system and its information.

#### Security Controls

47. A measure of the importance assigned to information by its owner, for the purpose of

denoting its need for protection.

### Sensitivity

48. Use of just one of the three available factors (something you know, something you have, something you are) to carry out the authentication process being requested.

### Single-Factor Authentication

49. The condition an entity is in at a point in time.

### State

50. The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

### System Integrity

51. Security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software or firmware components of the system.

### Technical Controls

52. Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image or reputation), organizational assets, individuals, other organizations or the nation through an information system via unauthorized access, destruction, disclosure, modification of information and/or denial of service.

### Threat

53. An individual or a group that attempts to exploit vulnerabilities to cause or force a threat to occur.

### Threat Actor



54. The means by which a threat actor carries out their objectives.

#### Threat Vector

55. A physical object a user possesses and controls that is used to authenticate the user's identity.

#### Token

56. Weakness in an information system, system security procedures, internal controls or implementation that could be exploited by a threat source.

#### Vulnerability

57. IEEE is a professional organization that sets standards for telecommunications, computer engineering and similar disciplines.

#### Institute of Electrical and Electronics Engineers

## **SECTION TWO: INCIDENT RESPONSE, DISASTER RECOVERY**

### Disaster Recovery Concepts

1. Events with a negative consequence, such as system crashes, network packet floods, unauthorized use of system privileges, defacement of a web page or execution of malicious code that destroys data.

#### Adverse Events

2. The loss of control, compromise, unauthorized disclosure, unauthorized acquisition or any similar occurrence where: a person other than an authorized user accesses or potentially accesses personally identifiable information; or an authorized user accesses personally identifiable information for other than an authorized purpose.

#### Breach

3. Actions, processes and tools for ensuring an organization can continue critical operations during a contingency.

## Business Continuity (BC)

4. The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption.

## Business Continuity Plan (BCP)

5. An analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.

## Business Impact Analysis (BIA)

6. In information systems terms, the activities necessary to restore IT and communications services to an organization during and after an outage, disruption or disturbance of any kind or scale.

## Disaster Recovery (DR)

7. The processes, policies and procedures related to preparing for recovery or continuation of an organization's critical business functions, technology infrastructure, systems and applications after the organization experiences a disaster. A disaster is when an organization's critical business function(s) cannot be performed at an acceptable level within a predetermined period following a disruption.

## Disaster Recovery Plan (DRP)

8. Any observable occurrence in a network or system.

## Event

9. A particular attack. It is named this way because these attacks exploit system vulnerabilities.

## Exploit

10. An event that actually or potentially jeopardizes the confidentiality, integrity or availability of an information system or the information the system processes, stores or transmits.

## Incident

11. The mitigation of violations of security policies and recommended practices.

## Incident Handling

12. The mitigation of violations of security policies and recommended practices.

## Incident Response (IR)

13. The documentation of a predetermined set of instructions or procedures to detect, respond to and limit consequences of a malicious cyberattack against an organization's information systems(s).

## Incident Response Plan (IRP)

14. A security event, or combination of security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system or system resource without authorization.

## Intrusion

15. A centralized organizational function fulfilled by an information security team that monitors, detects and analyzes events on the network or system to prevent and resolve issues before they result in business disruptions.

## Security Operations Center

16. Weakness in an information system, system security procedures, internal controls or implementation that could be exploited or triggered by a threat source.

## Vulnerability

17. A previously unknown system vulnerability with the potential of exploitation without risk of detection or prevention because it does not, in general, fit recognized patterns, signatures or methods.

### Zero Day

## **SECTION THREE: ACCESS CONTROL CONCEPTS**

1. Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures.

### Audit

2. An architectural approach to the design of buildings and spaces which emphasizes passive features to reduce the likelihood of criminal activity.

### Crime Prevention through Environmental Design (CPTED)

3. Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.

### Defense in Depth

4. A certain amount of access control is left to the discretion of the object's owner, or anyone else who is authorized to control the object's access. The owner can determine who should have access rights to an object and what those rights should be.

### Discretionary Access Control (DAC)

5. To protect private information by putting it into a form that can only be read by people who have permission to do so.

### Encrypt

6. Devices that enforce administrative security policies by filtering incoming traffic based on a set of rules.

### Firewalls

7. An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.

### Insider Threat

8. An operating system manufactured by Apple Inc. Used for mobile devices.

iOS

9. The use of multiple controls arranged in series to provide several consecutive controls to protect an asset; also called defense in depth.

Layered Defense

10. An operating system that is open source, making its source code legally available to end users.

Linux

11. A system irregularity that is identified when studying log entries which could represent events of interest for further surveillance.

Log Anomaly

12. Collecting and storing user activities in a log, which is a record of the events occurring within an organization's systems and networks.

Logging

13. An automated system that controls an individual's ability to access one or more computer system resources, such as a workstation, network, application or database. A logical access control system requires the validation of an individual's identity through some mechanism, such as a PIN, card, biometric or other token. It has the capability to assign different access privileges to different individuals depending on their roles and responsibilities in an organization.

Logical Access Control Systems

14. Access control that requires the system itself to manage access controls in accordance with the organization's security policies.

Mandatory Access Control

15. An entrance to a building or an area that requires people to pass through two doors with only one door opened at a time.

#### Mantrap

16. Passive information system-related entity (e.g., devices, files, records, tables, processes, programs, domains) containing or receiving information. Access to an object (by a subject) implies access to the information it contains. See subject.

#### Object

17. Controls implemented through a tangible mechanism. Examples include walls, fences, guards, locks, etc. In modern organizations, many physical control systems are linked to technical/logical systems, such as badge readers connected to door locks.

#### Physical Access Controls

18. The principle that users and programs should have only the minimum privileges necessary to complete their tasks.

#### Principle of Least Privilege

19. An information system account with approved authorizations of a privileged user.

#### Privileged Account

20. A type of malicious software that locks the computer screen or files, thus preventing or limiting a user from accessing their system and data until money is paid.

#### Ransomware

21. An access control system that sets up user permissions based on roles.

#### Role-based access control (RBAC)

22. An instruction developed to allow or deny access to a system by comparing the validated identity of the subject to an access control list.

#### Rule

23. The practice of ensuring that an organizational process cannot be completed by a single person; forces collusion as a means to reduce insider threats. Also commonly known as Separation of Duties.

#### Segregation of Duties

24. Generally an individual, process or device causing information to flow among objects or change to the system state.

#### Subject

25. The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software or firmware components of the system.

#### Technical Controls

26. A one-way spinning door or barrier that allows only one person at a time to enter a building or pass through an area.

#### Turnstile

27. An operating system used in software development.

#### Unix

28. The process of creating, maintaining and deactivating user identities on a system.

#### User Provisioning

### **SECTION FOUR - NETWORK SECURITY**

1. A set of routines, standards, protocols, and tools for building software applications to access a web-based software application or web tool.

#### Application programming interface (API)

2. The most essential representation of data (zero or one) at Layer 1 of the Open Systems Interconnection (OSI) model.

#### Bit

3. Broadcast transmission is a one-to-many (one-to-everyone) form of sending internet traffic.

#### Broadcast

4. The byte is a unit of digital information that most commonly consists of eight bits.

#### Byte

5. 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.

#### Cloud Computing

6. A system in which the cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy and compliance considerations). It may be owned, managed and operated by one or more of the organizations in the community, a third party or some combination of them, and it may exist on or off premises.

#### Community Cloud

7. The opposite process of encapsulation, in which bundles of data are unpacked or revealed.

#### De-encapsulation

8. The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.)

#### Denial-of-Service (DoS)



9. This acronym can be applied to three interrelated elements: a service, a physical server and a network protocol.

#### Domain Name Service (DNS)

10. Enforcement of data hiding and code hiding during all phases of software development and operational use. Bundling together data and methods is the process of encapsulation; its opposite process may be called unpacking, revealing, or using other terms. Also used to refer to taking any set of data and packaging it or hiding it in another data structure, as is common in network protocols and encryption.

#### Encapsulation

11. The process and act of converting the message from its plaintext to ciphertext. Sometimes it is also referred to as enciphering. The two terms are sometimes used interchangeably in literature and have similar meanings.

#### Encryption

12. The internet protocol (and program) used to transfer files between hosts.

#### File Transfer Protocol (FTP)

13. In a fragment attack, an attacker fragments traffic in such a way that a system is unable to put data packets back together.

#### Fragment attack

14. The physical parts of a computer and related devices.

#### Hardware

15. A combination of public cloud storage and private cloud storage where some critical data resides in the enterprise's private cloud while other data is stored and accessible from a public cloud storage provider.

#### Hybrid cloud

16. The provider of the core computing, storage and network hardware and software that is the foundation upon which organizations can build and then deploy applications. IaaS is popular in the data center where software and servers are purchased as a fully outsourced service and usually billed on usage and how much of the resource is used.

#### Infrastructure as a Service (IaaS)

17. An IP network protocol standardized by the Internet Engineering Task Force (IETF) through RFC 792 to determine if a particular service or host is available. Internet Control Message Protocol (ICMP)

18. Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks.

Internet Protocol (IPv4)

19. An attack where the adversary positions himself in between the user and the system so that he can intercept and alter data traveling between them.

Man-in-the-Middle

20. Part of a zero-trust strategy that breaks LANs into very small, highly localized zones using firewalls or similar technologies. At the limit, this places a firewall at every connection point.

Microsegmentation

21. Purposely sending a network packet that is larger than expected or larger than can be handled by the receiving system, causing the receiving system to fail unexpectedly.

Oversized Packet Attack

22. Representation of data at Layer 3 of the Open Systems Interconnection (OSI) model.

Packet

23. The primary action of a malicious code attack.

Payload

24. An information security standard administered by the Payment Card Industry Security Standards Council that applies to merchants and service providers who process credit or debit card transactions.

Payment Card Industry Data Security Standard (PCI DSS)

25. The web-authoring or application development middleware environment that allows applications to be built in the cloud before they're deployed as SaaS assets.

Platform as a Service (PaaS)

26. The phrase used to describe a cloud computing platform that is implemented within the corporate firewall, under the control of the IT department. A private cloud is designed to offer the same features and benefits of cloud systems, but removes a number of objections to the cloud computing model, including control over enterprise and customer data, worries about security, and issues connected to regulatory compliance.

#### Private cloud

27. A set of rules (formats and procedures) to implement and control some type of association (that is, communication) between systems.

#### Protocols

28. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

#### Public cloud

29. The standard communication protocol for sending and receiving emails between senders and receivers.

#### Simple Mail Transport Protocol (SMTP)

30. Computer programs and associated data that may be dynamically written or modified during execution.

#### Software

31. The cloud customer uses the cloud provider's applications running within a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

#### Software as a Service (SaaS)

32. Faking the sending address of a transmission to gain illegal entry into a secure system

#### Spoofing

33. Internetworking protocol model created by the IETF, which specifies four layers of functionality: Link layer (physical communications), Internet Layer (network-to-network communication), Transport Layer (basic channels for connections and connectionless exchange of data between hosts), and Application Layer, where other protocols and user applications programs make use of network services.

## Transport Control Protocol/Internet Protocol (TCP/IP) Model

34. A virtual local area network (VLAN) is a logical group of workstations, servers, and network devices that appear to be on the same LAN despite their geographical distribution.

### VLAN

35. A virtual private network (VPN), built on top of existing networks, that can provide a secure communications mechanism for transmission between networks.

### VPN

36. A wireless area network (WLAN) is a group of computers and devices that are located in the same vicinity, forming a network based on radio transmissions rather than wired connections. A Wi-Fi network is a type of WLAN.

### WLAN

37. The graphical user interface (GUI) for the Nmap Security Scanner, an open-source application that scans networks to determine everything that is connected as well as other information.

### Zenmap

38. Removing the design belief that the network has any trusted space. Security is managed at each possible level, representing the most granular asset. Microsegmentation of workloads is a tool of the model.

### Zero Trust

## **SECTION FIVE: SECURITY OPERATIONS**

1. A computer responsible for hosting applications to user workstations.

### Application Server

2. An algorithm that uses one key to encrypt and a different key to decrypt the input plaintext.

### Asymmetric Encryption

3. A digit representing the sum of the correct digits in a piece of stored or transmitted digital data, against which later comparisons can be made to detect errors in the data.

### Checksum

4. The altered form of a plaintext message so it is unreadable for anyone except the intended recipients. In other words, it has been turned into a secret.

### Ciphertext

5. Classification identifies the degree of harm to the organization, its stakeholders or others that might result if an information asset is divulged to an unauthorized person, process or organization. In short, classification is focused first and foremost on maintaining the confidentiality of the data, based on the data sensitivity.

### Classification

6. A process and discipline used to ensure that the only changes made to a system are those that have been authorized and validated.

### Configuration management

7. One who performs cryptanalysis which is the study of mathematical techniques for attempting to defeat cryptographic techniques and/or information systems security. This includes the process of looking for errors or weaknesses in the implementation of an algorithm or of the algorithm itself.

### Cryptanalyst

8. The study or applications of methods to secure or protect the meaning and content of messages, files, or other information, usually by disguise, obscuration, or other transformations of that content and meaning.

### Cryptography

9. System capabilities designed to detect and prevent the unauthorized use and transmission of information.

### Data Loss Prevention (DLP)

10. The reverse process from encryption. It is the process of converting a ciphertext message back into plaintext through the use of the cryptographic algorithm and the appropriate key for decryption (which is the same for symmetric encryption, but different for asymmetric encryption). This term is also used interchangeably with the "deciphering."

### Decryption

11. A technique of erasing data on disk or tape (including video tapes) that, when performed properly, ensures that there is insufficient magnetic remanence to reconstruct data.

### Degaussing

12. The result of a cryptographic transformation of data which, when properly implemented, provides the services of origin authentication, data integrity, and signer non-repudiation.

### Digital Signature

13. Monitoring of outgoing network traffic.

### Egress Monitoring

14. The process and act of converting the message from its plaintext to ciphertext. Sometimes it is also referred to as enciphering. The two terms are sometimes used interchangeably in literature and have similar meanings.

### Encryption

15. The total set of algorithms, processes, hardware, software, and procedures that taken together provide an encryption and decryption capability.

### Encryption System

16. A reference to the process of applying secure configurations (to reduce the attack surface) and locking down various hardware, communications systems, and software, including operating system, web server, application server, application, etc. Hardening is normally performed based on industry guidelines and benchmarks, such as those provided by the Center for Internet Security (CIS).

### Hardening

17. An algorithm that computes a numerical value (called the hash value) on a data file or electronic message that is used to represent that file or message and depends on the entire contents of the file or message. A hash function can be considered to be a fingerprint of the file or message.

### Hash Function

18. The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data.

### Hashing

19. The requirements for information sharing by an IT system with one or more other IT systems or applications, for information sharing to support multiple internal or external organizations, missions, or public programs.

#### Information Sharing

20. Monitoring of incoming network traffic.

#### Ingress Monitoring

21. A digital signature that uniquely identifies data and has the property such that changing a single bit in the data will cause a completely different message digest to be generated.

#### Message Digest

22. The software "master control application" that runs the computer. It is the first program loaded when the computer is turned on, and its main component, the kernel, resides in memory at all times. The operating system sets the standards for all application programs (such as the Web server) that run in the computer. The applications communicate with the operating system for most user interface and file management operations.

#### Operating System

23. A software component that, when installed, directly modifies files or device settings related to a different software component without changing the version number or release details for the related software component.

#### Patch

24. The systematic notification, identification, deployment, installation and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs.

#### Patch Management

25. A message or data in its natural format and in readable form; extremely vulnerable from a confidentiality perspective.

#### Plaintext

26. The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).

#### Records

27. A practice based on the records life cycle, according to which records are retained as long as necessary, and then are destroyed after the appropriate time interval has elapsed.

#### Records Retention

28. Residual information remaining on storage media after clearing.

#### Remanence

29. The first stage of change management, wherein a change in procedure or product is sought by a stakeholder.

#### Request for change (RFC)

30. The entirety of the policies, roles, and processes the organization uses to make security decisions in an organization.

#### Security Governance

31. Tactics to infiltrate systems via email, phone, text, or social media, often impersonating a person or agency in authority or offering a gift. A low-tech method would be simply following someone into a secure building.

#### Social engineering

32. An algorithm that uses the same key in both the encryption and the decryption processes.

#### Symmetric encryption

33. A computer that provides World Wide Web (WWW) services on the Internet. It includes the hardware, operating system, Web server software, and Web site content (Web pages). If the Web server is used internally and not by the public, it may be known as an "intranet server."

#### Web Server



## **CONCLUSION**

Cybersecurity is vital in today's interconnected world, where threats to information and systems are constant and evolving. Understanding and implementing effective security principles safeguard not only sensitive data but also the trust and functionality essential to organizations and individuals alike. By staying informed and proactive, we build resilience against risks and ensure a more secure digital future.

Idea Sheets provide quick and actionable suggestions to drive more referrals and sales. Visit [www.referralsafe.com/asktra](http://www.referralsafe.com/asktra) frequently for new additions.