Cybersecurity glossary
Antivirus
Software designed to prevent viruses entering a computer system or network.

Access Control Mechanism
Security measures designed to detect and deny unauthorised access and permit authorised access to an information system or a physical facility.

Adversary
An individual, group, organisation, or government that conducts (or intends to conduct) detrimental activities.

Asset
Something of value. This could be a person, structure or facility, information, systems and resources, materials, processes, relationships, or reputation.

Attack
An attempt to gain unauthorised access to system services, resources, or information, or to compromise system integrity.

Attacker
An individual, group, organisation, or government that executes an attack. A party acting with malicious intent to compromise an information system.

Authentication
The process of verifying the identity or other attributes of an entity (user, process, or device).

Behaviour Monitoring
Observing activities of users, information systems, and processes and measuring the activities against organisational policies, baselines of normal activity, thresholds, and trends.

Blacklist
A list of entities that are blocked or denied privileges or access.

Bot
A computer connected to the Internet that has been surreptitiously compromised with malicious logic to perform activities under the command and control of a remote administrator.

Botnet
A collection of computers compromised by malicious code, and controlled across a network.

Bug
An unexpected and relatively small defect, fault, flaw, or imperfection in an information system or device.

Ciphertext
Data or information in its encrypted form.

Cloud Computing
A model for enabling on-demand network access to a shared pool of configurable computing capabilities or resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Computer Network Defence
The actions taken to defend against unauthorised activity within computer networks.

Confidentiality
Authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Cryptanalysis
The operations performed in defeating or circumventing cryptographic protection of information by applying mathematical techniques.

Cryptography
The use of mathematical techniques to provide security services, such as confidentiality, data integrity, entity authentication, and data origin authentication.

The art or science concerning the principles, means, and methods for converting plaintext into ciphertext and for restoring encrypted ciphertext to plaintext.

Cryptology
The mathematical science that deals with cryptanalysis and cryptography.

Cyber Ecosystem
The interconnected information infrastructure of interactions among persons, processes, data, and information and communications technologies, along with the environment and conditions that influence those interactions.

Cybersecurity
The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorised use or modification, or exploitation.

Cybersecurity glossary
Data Breach
The unauthorised movement or disclosure of sensitive information to a party, usually outside the organisation, that is not authorised to have or see the information.

Data Integrity
Data that is complete, intact, and trusted and has not been modified or destroyed in an unauthorised or accidental manner.

Data Loss
The result of unintentionally or accidentally deleting data, forgetting where it is stored, or exposure to an unauthorised party.

Data Mining
The process or techniques used to analyse large sets of existing information to discover previously unrevealed patterns or correlations.

Data Theft
The deliberate or intentional act of stealing of information.

Decipher
To convert enciphered text to plaintext by means of a cryptographic system.

Denial of Service
An attack that prevents or impairs the authorised use of information system resources or services.

Digital Forensics
The processes and specialised techniques for gathering, retaining, and analysing system-related data (digital evidence) for investigative purposes.

Digital Signature
A value computed with a cryptographic process using a private key and then appended to a data object, thereby digitally signing the data.

Disruption
An event that causes unplanned interruption in operations or functions for an unacceptable length of time.

Distributed Denial of Service (DDoS)
A distributed denial-of-service (DDoS) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system.

Electronic Signature
Any mark in electronic form associated with an electronic document, applied with the intent to sign the document.

Encipher
To convert plaintext to ciphertext by means of a cryptographic system.

Encode
To convert plaintext to ciphertext by means of a code.

Encryption
The process of transforming plaintext into ciphertext.

Converting data into a form that cannot be easily understood by unauthorised people.

Exploit
A technique to breach the security of a network or information system in violation of security policy.

Exposure
The condition of being unprotected, thereby allowing access to information or access to capabilities that an attacker can use to enter a system or network.

Failure
The inability of a system or component to perform its required functions within specified performance requirements.

Firewall
A capability to limit network traffic between networks and/or information systems.
Hacker
An unauthorised user who attempts to or gains access to an information system.

Hashing
A process of applying a mathematical algorithm against a set of data to produce a numeric value (a ‘hash value’) that represents the data.

Identity and Access Management
The methods and processes used to manage subjects, authentication, and access to specific objects (systems, networks, devices).

Incident
An occurrence may result in adverse consequences to an information system or the information that the system processes, stores, or transmits.

An occurrence that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Incident Management
The management and coordination of activities associated with an event that may result in adverse consequences to information or information systems.

Incident Response
The activities that address the short-term, direct effects of an incident and may also support short-term recovery.

Incident Response Plan
A set of predetermined and documented procedures to detect and respond to a cyber incident.

Information Security Policy
Regulations, rules, and practices that prescribe how an organisation manages, protects, and distributes information.

Inside(r) Threat
A person or group of persons within an organisation who pose a potential risk through violating security policies.

Integrity
The property whereby information, an information system, or a component of a system has not been modified or destroyed in an unauthorised manner.

Interoperability
The ability of two or more systems or components to exchange information.

Intrusion
An unauthorised act of bypassing the security mechanisms of a network or information system.

Intrusion Detection
The process and methods for analysing information from networks and information systems to determine if a security breach or security violation has occurred.

Investigation
A systematic and formal inquiry into a qualified threat or incident using digital forensics to determine the events that transpired, and to collect evidence.
Key
The numerical value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification.

Keylogger
Software or hardware that tracks keystrokes and keyboard events to monitor actions by the user of an information system.

Macro Virus
A type of malicious code that attaches itself to documents and uses the macro programming capabilities of the document’s application to execute, replicate, and spread or propagate itself.

Malicious Code
Program code intended to perform an unauthorised function or process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This may include software, firmware, and scripts.

Malicious Logic
Hardware, firmware, or software that is intentionally included or inserted in a system to perform an unauthorised function or process that will have adverse impact on the confidentiality, integrity, or availability of an information system.

Malware
Software that compromises the operation of a system by performing an unauthorised function or process.

Man-In-The-Middle (MITM) Attack
When a hacker intercepts communication between two (or more) parties and relays the information to both sides.

Mitigation
The application of one or more measures to reduce the likelihood of an unwanted occurrence and/or lessen its consequences.

Network Resilience
The ability of a network to:
1. Provide continuous operation (i.e., highly resistant to disruption and able to operate in a degraded mode if damaged);
2. Recover effectively if failure does occur; and
3. Scale to meet rapid or unpredictable demands.
Operational Exercise
An action-based exercise where personnel rehearse reactions to an incident scenario, drawing on their understanding of plans and procedures, roles, and responsibilities.

Operations Technology
The hardware and software systems used to operate industrial control devices.

Outside(rnd) Threat
A person or group of persons external to an organisation who are not authorised to access its assets and pose a potential risk to the organisation.

Passive Attack
An assault perpetrated by an intentional threat source that attempts to learn or make use of information from a system, but does not attempt to alter the system, its resources, its data, or its operations.

Password
A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorisation.

Pen Test
A colloquial term for ‘penetration test’ or ‘penetration testing’ – an evaluation methodology whereby assessors search for vulnerabilities and attempt to circumvent the security features of a network and/or information system.

Personal Identifying Information / Personally Identifiable Information
The information that permits the identity of an individual to be directly or indirectly inferred.

Phishing
The attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

Plaintext
Unencrypted information.

Privacy
The assurance that the confidentiality of, and access to, certain information about an entity is protected.

Private Key
A cryptographic key that must be kept confidential and is used to enable the operation of an asymmetric (public key) cryptographic algorithm.

Public Key
A cryptographic key that can be obtained and used by anyone to encrypt messages intended for a particular recipient, such that the encrypted messages can be deciphered only by using a second key that is known only to the recipient (the private key).

Ransomware
Ransomware is a form of computer malware that can be easily installed covertly on a victim’s computer. Ransomware prevents a user from being able to operate their PC normally unless they comply with the demands of the attacker. To regain access to your PC and files, you typically have pay money – a ‘ransom’ – to the attacker in exchange for unlocking your system.

Recovery
The activities after an incident or event to restore essential services and operations in the short and medium term, and fully restore all capabilities in the longer term.

Redundancy
Additional or alternative systems, sub-systems, assets, or processes that maintain a degree of overall functionality in case of loss or failure of another system, sub-system, asset, or process.

Resilience
The ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption.

Response
The activities that address the short-term, direct effects of an incident and may also support short-term recovery.

Risk
The potential for an unwanted or adverse outcome resulting from an incident, event, or occurrence, as determined by the likelihood that a threat will exploit a vulnerability.

Risk Assessment
The product or process that collects information and assigns values to risks for informing priorities, developing or comparing courses of action, and informing decision making.

Risk Management
The process of identifying, analysing, assessing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level considering associated costs and benefits of any actions taken.
| **Secret Key** | A cryptographic key that is used for both encryption and decryption, enabling the operation of a symmetric key cryptography scheme. |
| **Securely Provision** | Conceptualising, designing, and building secure IT systems. |
| **Security Automation** | The use of information technology in place of manual processes for cyber incident response and management. |
| **Security Policy** | A rule or set of rules that govern the acceptable use of an organisation’s information and services to a level of acceptable risk and the means for protecting the organisation’s information assets. |
| **Signature** | A recognisable, distinguishing pattern. |
| **Software Assurance** | The level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its lifecycle, and that the software functions in the intended manner. |
| **Spam** | The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages. |
| **Spoofing** | Faking the sending address of a transmission to gain unauthorised entry into a secure system. |
| **Spyware** | Software that is secretly installed into an information system without the knowledge of the system user or owner. |
| **SQL Injection** | A Structured Query Language (SQL) injection attack targets back-end databases and applications that use the SQL programming language. SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server. |
| **Symmetric Key** | A cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt plaintext and decrypt ciphertext, or create a message authentication code and to verify the code. |
| **System Administration** | Where a person installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure confidentiality, integrity, and availability. |
| **System Integrity** | The attribute of an information system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorised manipulation of the system. |
| **Systems Security Architecture** | Where a person develops system concepts and works on the capabilities phases of the systems development lifecycle; translates technology and environmental conditions into system and security designs and processes. |
| **Threat** | A circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact organisational operations, assets (including information and information systems), individuals, other organisations, or society. |
| **Threat Agent** | An individual, group, organisation, or government that conducts or has the intent to conduct detrimental activities. |
| **Threat Analysis** | The detailed evaluation of the characteristics of individual threats. |
| **Threat Assessment** | The product or process of identifying or evaluating entities, actions, or occurrences, whether natural or man-made, that have or indicate the potential to cause harm. |
| **Trojan Horse** | A computer program that has a hidden malicious function that evades security mechanisms, sometimes by exploiting legitimate authorisations of a system entity that invokes the program. |
Unauthorised Access
Any access that violates the stated security policy.

Weakness
A shortcoming or imperfection in software code, design, architecture, or deployment that, under proper conditions, could become a vulnerability or contribute to the introduction of vulnerabilities.

Whitelist
A list of entities that are considered trustworthy and are granted access or privileges.

Worm
A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.

Virus
A computer program that can replicate itself, infect a computer without permission or knowledge of the user, and then spread or propagate to another computer.

Vulnerability
A characteristic or specific weakness that renders an organisation or asset (such as information or an information system) open to exploitation by a given threat or susceptible to a given hazard.

Zero Day Vulnerability
A hole in software, unknown to the vendor or general public, that is exploited by hackers.
Is cybersecurity a top priority?

Ours too. As part of a global network of centres, find out how the new Australian Advanced Security Operation Centre can work with your business to protect against cyber-crime and reinstate innovation as your business’ top priority.

Visit optus.com.au/business/asoc to book a free tour
To discuss how Optus can help you through advanced security solutions, contact your Optus Account Manager or call the Optus Business hotline on 1800 555 937

Join the conversation

1800 555 937  optus.com.au/business  @optusbusiness  yesopt.us/blog  bit.ly/OBLinkedIn

Give us a call