GLOSSARY OF INFORMATION
SECURITY TERMS

Access: The ability to obtain, examine, or retrieve an information technology resource.

Access control: A combination of policies, models, and mechanisms that regulate access to system resources and protect system resources against unauthorized user access. Mechanisms include software, biometrics devices, and physical security measures.

Access point (AP): A device that logically connects wireless client devices operating in infrastructure to one another and provides access to a distribution system, if connected, which is typically an organization's enterprise wired network.

Active attack: An intentional attempt to alter, disable, or destroy a system, its operations, resources, or data. Typically the attack is on the authentication protocol of a system.

Administrator account: A user account with credentials that confer full privileges on a computer and/or throughout a network.

Advanced encryption standard (AES): Algorithm used to protect electronic data through a symmetric block cipher. AES is approved by the United States government to protect electronic data.

Advanced persistent threats (APT): A covert network attack, usually through multiple attack vectors (e.g., cyber, physical, and deception) and often occurring over an extended period of time. The attackers generally seek to establish footholds in the organization's IT infrastructure to wage future attacks.

Advanced threat protection (ATP): A category of security solutions that defend against sophisticated malware or hacking-based attacks targeting sensitive data. Advanced threat protection solutions can be available as software or as managed services. ATP solutions can differ in approaches and components, but most include some combination of endpoint agents, network devices, email gateways, malware protection systems, and a centralized management console to correlate alerts and manage defenses.

Antispyware software: A type of program designed to prevent and detect unwanted spyware program installations and to remove those programs if installed.

Antivirus: Software used to prevent, detect, and remove malicious applications such as computer worms, viruses, and Trojan horses **f**rom systems, servers, and endpoints. Once an infected file has been detected, it can be either repaired or quarantined so that the viral code does not execute. When a new virus is discovered, a unique string of code is extracted and added to a database with other information about the virus.

Attack attribution: Determining the identity or location of an attacker or the attacker's intermediary.

Attack sensing and warning (AS&W): Detection, correlation, identification, and characterization of intentional unauthorized activity with notification to decision makers so that an appropriate response can be developed.

Attack signature: Rules or patterns in the heading of a packet or in the pattern of a group of packets that distinguish legitimate traffic from attacks or classes of attacks on a web application and its components.

Authentication: Method to verify credentials through passwords, biometrics, one-time pins, or apps and data typically moved through ID tokens.

Authorization: The granting or denying of access rights to a user, program, or process.

Attribute-based access control (ABAC): An access control approach in which access is mediated based on attributes associated with subjects (requesters) and the objects to be accessed. Each object and subject has a set of associated attributes, such as location, time of creation, access rights, etc. Access to an object is authorized or denied depending upon whether the required (e.g., policy-defined) correlation can be made between the attributes of that object and of the requesting subject.

Back door: Typically unauthorized hidden software or hardware mechanism used to circumvent security controls to gain access to a computer system.

Basic input/output system (BIOS): Refers collectively to boot firmware based on the conventional BIOS, Extensible Firmware Interface (EFI), and the Unified Extensible Firmware Interface (UEFI).

Beyond corp: is an implementation, by Google, of zero-trust computer security concepts creating a zero trust network.

Biometrics: The science and technology of measuring and analyzing biological data. The term usually refers to automated technologies for authenticating users through characteristics such as fingerprints, eye retinas or irises, voice patterns, facial patterns, and hand measurements.

Blacklist: A list of people or programs that are blocked or denied privileges within or access to a system or service.

Blue team: A group of individuals who perform an analysis of information systems to ensure security, identify security flaws, verify the effectiveness of each security measure, and to make certain all security measures will continue to be effective after implementation.

Botnet: A network of hundreds or thousands of computers infected with malicious code that work together to perform tasks assigned by the network controller. These tasks are either automated or assigned through a control channel such as internet relay chat.

Brute force attack: A method of accessing a computer or network by attempting multiple combinations of numeric and/or alphanumeric passwords.

Buffer overflow attack: A method of accessing a computer or network by sending more input than can be placed into a buffer or data holding area to crash a system or to insert specially crafted code that allows the attacker to gain control of the system.

Business continuity plan (BCP): A plan to help ensure that business processes can continue during an emergency or disaster. In the context of information security, the plan will detail the restoration of critical IT processes and operations as well as design an architecture that prevents, detects, and isolates security breaches and reroutes network traffic in the event of a circuit failure.

Business impact analysis (BIA): 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.

Category: A restrictive label that can be applied to classified or unclassified information to limit access or to trigger heightened security measures.

Certificate: A set of data that uniquely identifies an organization, contains the organization's public key and possibly other information, and is digitally signed by a trusted party, thereby binding the public key to the organization.

Certification authority revocation list (CARL): A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates, that have been revoked.

Clear text: Information that is not encrypted.

Client: A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server.

Cloud access security brokers (CASB): Software or hardware that works in-between the cloud users and cloud providers to monitor activity and apply security policies of organization. May be cloud based or on-premise (on-prem).

Cloud computing: Technology that uses the internet and shared central remote servers, rather than local servers or personal devices, to store data and applications. Centralizing data storage, processing, and bandwidth improves efficiency.

Commercial-off-the-shelf (COTS): Software and hardware that already exists and is available from commercial sources. It is also referred to as off-the-shelf.

Common security control: Security control that can be applied to one or more agency information systems and has the following properties: (i) the development, implementation, and assessment of the control can be assigned to a responsible official or organizational element (other than the information system owner); and (ii) the results from the assessment of the control can be used to support the security certification and accreditation processes of an agency information system where that control has been applied.

Compartmentalization: Organizing resources into groups that are isolated from each other and controlling the means of exchanging information between groups. When networks are compartmentalized, filtering devices such as firewalls are used to partition a network into zones.

Compensating controls: The security and privacy controls implemented in lieu of the controls in the baselines described within the applicable standard (ISO 27001, NIST SP 800, HITRUST, SOC II, PCI).

Computer security incident: Any unlawful, unauthorized, or unacceptable action that involves a computer system or computer network. This can include theft of trade secrets, email spam, unauthorized intrusions into computing systems, or denial-of-service attacks (DDOS).

Containers: Isolated user-space instances that share an operating system kernel and may share files as well.

Corrective action plan (CAP): Corrective actions for an issuer for removing or reducing deficiencies or risks identified by the Assessor during the assessment of issuer operations. The plan identifies actions that need to be performed in order to obtain or sustain authorization.

Credentials: A data object that supports a claim of identity or authorization that is generally intended to be used more than once.

Credential service provider (CSP): A trusted entity that issues or registers subscriber tokens and issues electronic credentials to subscribers. The CSP may encompass registration authorities (RAs) and verifiers that it operates. A CSP may be an independent third party, or may issue credentials for its own use.

Cross-site scripting (XSS): A prevalent security vulnerability in websites and web applications where data that is inputted by a user is sent to the browser without proper validation or sanitation. In an XSS attack, an attacker exploits this vulnerability by inputting malicious code, which is injected on the website. Users become victims by visiting or clicking on a link to the compromised website. Injected code may cause the

compromised website to display inappropriate images, redirect users to a malicious website, or cause malicious files to be automatically downloaded onto a user's computer.

Cybersecurity: Protects, restores, and prevents damage to information technology devices, electronic communications, and electronic communications services, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Data breach: This term is defined differently under various laws and regulations, but generally it is the unauthorized disclosure of sensitive or privileged information to a party that is not authorized to access the information.

Data integrity: The process of preventing accidental deletion or corruption of data in a database.

Data loss prevention (DLP): A strategy for preventing data loss due to insider threats by ensuring end users cannot send or otherwise share confidential information outside of the corporate network.

Data mining: The process of analyzing large amounts of data, usually through an automated process, to uncover facts, patterns, relationships, trends, and anomalies with the goal of using the information to predict data subjects' behavior.

Defense-in-depth: A comprehensive security strategy involving the coordinated use of multiple security countermeasures utilizing technology, people, and operational capabilities to protect the integrity of an organization's information assets.

Demilitarized zone (DMZ): Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network’s Information Assurance policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.

Digital forensics: The specialized techniques used to collect, retain, and analyze potential evidence in digital form for investigative purposes, preserving and proving chain of custody, and providing expert testimony.

Digital rights management: Any access control technology used to protect, license, and otherwise restrict the use of proprietary software, hardware, or content.

Digital signature: A data string that is added to a digital message to guarantee its integrity and validate the message's origin. The string is created by hashing the original message into a few lines, known as a message digest, and then encrypting it with the signatory's private key. Message recipients can determine whether a message has been modified by hashing it into a message digest, decrypting the signature with the sender's public key, and comparing the two message digests.

Disaster Recovery Plan (DRP): A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.

Disruption: An event that causes an unscheduled interruption in processes or operations of systems or applications for an unusual or unacceptable length of time.

Distributed denial of service attack (DDoS): The introduction of code into a trusted component or software that will be distributed to other computers. The infected computers can then be instructed remotely to send a flood of network traffic to a target. Overwhelming the target system causes delays and outages, thus making its resources, websites, applications, email, voicemail,
etc. unavailable to legitimate users.

Domain Controller: A server responsible for managing domain information, such as login identification and passwords.

Encryption: Encoding information and messages so they are unusable, unreadable, or indecipherable without providing the reader a key or password.

End-to-end security: Safeguarding information in an information system from point of origin to point of destination.

Enterprise: An organization such as a business or company.

Enterprise risk management: The process of planning, organizing, leading, and controlling the activities of an organization to minimize the risk to its assets. Typically an enterprise will identify its capabilities and dependencies and create countermeasures to protect risks to those identified assets.

Exploit: A method or a program that automates a method that targets a software vulnerability to compromise the integrity, availability, or confidentiality of information or services.

Failover: The capability to switch over automatically (typically without human intervention or warning) to a redundant or standby information system upon the failure or abnormal termination of the previously active system.

Federated identity: The means of linking a person's electronic identity and attributes, stored across multiple distinct identity management systems. SSO is a subset of federated identity management.

File transfer protocol (FTP): FTP is an Internet standard for transferring files over the Internet. FTP programs and utilities are used to upload and download Web pages, graphics, and other files between local media and a remote server which allows FTP access.

Firewall: Software applications on a network gateway server that are used to keep a network secure. A firewall can be used to separate internal network segments and public web servers to prevent unauthorized access to private network resources from outside the network. A firewall can also be used to protect internal network segments from unauthorized use by someone within the network.

Forensics: A structured investigation of computer systems, networks, wireless communications, and storage devices to identify, collect, preserve the integrity of, and analyze data that can be presented as evidence in court.

Gigabyte: One thousand megabytes.

Governance risk and compliance (GRC): Software solutions addressing three related facets that aim to assure an organization reliably achieves objectives, addresses uncertainty and acts with integrity.

Hardware security module (HSM): A physical computing device that safeguards and manages cryptographic keys and provides cryptographic processing. An HSM is or contains a cryptographic module.

Hashed: The process whereby data (e.g., a message) was input to a cryptographic hash function to produce a hash value.

Honeypot: A system or system resource created to attract potential intruders. The goal is to distract intruders from the real target and to gain information about the intruder and the attack.

Identity access management (IAM): *A* system of managing access to information and applications in internal and external applications systems. IAM generally has four components: authentication, authorization, user management, and a central user repository that stores and delivers identity information to services and verifies credentials submitted by users.

Incident response plan (IRP): A process or set of activities including impact and scope measurement and remediation that addresses the immediate and direct effects of a cyber incident and provides short-term recovery*.*

Incident response team (IRT): Group of people who prepare for and respond to any emergency incident, such as a natural disaster or an interruption of business operations. Incident response teams are common in public service organizations as well as in other organizations, either military or specialty.

Insider threat: A threat that originates within an organization and threatens to use authorized access, willingly or otherwise, to harm an organization through system or data modification, disclosure, destruction, or suspension of service.

Intrusion prevention system (IPS): A device or software used to prevent intruders from accessing systems and halt malicious or suspicious activity. An IPS will identify malicious activity, log information about it, attempt to stop it, and report it. This is in contrast to an intrusion detection system, which merely detects and notifies but takes no further action.

Investigation: A systematic inquiry into a threat or incident using digital forensics and other examination techniques to collect evidence and determine specifically what has transpired.

Internet protocol (IP) address: A unique number that devices use to identify and communicate with one another on a computer network using the IP standard. All devices on a network, including routers, computers, printers, and internet fax machines, must have their own IP addresses. This is the standard protocol for data transmission.

Intrusion: A security event or events where an unauthorized entity gains or attempts to gain access to a system or system resource, without authorization, by circumventing the system's security protections.

Javascript (Java): Scripting language utilized largely in website design and website applications. Key: A string of bits used by an algorithm to produce encrypted text from a string of unencrypted text or to produce decrypted text from a string of encrypted text.

Local area network (LAN): A group of computers and associated devices that are connected to the same server by hardware and software communications facilities to share resources, such as information, and peripheral devices, such as printers and modems. Typically the devices and server are all in a small geographic area.

Log: Record of what has occurred within an information technology system or within a network. Typically kept by the system administrator or IT department.

Malware: Malicious software intended to do harm, such as disrupting computer operations, stealing confidential information, or gaining access to computer systems. Malware includes viruses, ransomware, worms, Trojan horses, rootkits, keyloggers, spyware, malicious mobile code, and browser helper objects.

Managed security service provider (MSSP): Service involves installing, upgrading, and managing the firewall, Virtual Private Network (VPN) and/or intrusion detection hardware and software, electronic mail, and commonly performing configuration changes on behalf of the customer. Management includes monitoring, maintaining the firewall's traffic routing rules, and generating regular traffic and management reports to the customer.[1] Intrusion detection management, either at the network level or at the individual host level, involves providing intrusion alerts to a customer, keeping up to date with new defenses against intrusion, and regularly reporting on intrusion attempts and activity. Content filtering services may be provided by; such as, email filtering and other data traffic filtering.

Man-in-the-middle attack: A form of attack when an attacker intercepts and modifies data in order to deceive parties to a conversation into thinking they are conversing with each other while they are really conversing with the attacker.

Mobile devices management (MDM): Administration of mobile devices, such as smartphones, tablet computers and laptops. MDM is usually implemented with the use of a third-party product that has management features for particular vendors of mobile devices.

Multi-factor authentication (MFA): A type of authentication based on more than one component. For example, something a user knows, such as a password, would serve as one component and would be combined with another component, such as something the user is, such as a fingerprint, or something the user has, such as a debit card or authentication device. To access a network, the user must have all the required components.

Network: A group of computers and associated devices that are interconnected by hardware and software communications facilities in order to share resources, such as information, and peripheral devices, such as printers and modems.

Network-based incident response: A set of disciplines, technologies, and processes for responding to incidents that focuses on attempts to block breaches at the network perimeter or firewall.

Network interface card (NIC): A circuit board or card that is installed in a computer so that it can be connected to a network.

OAuth: An open standard for access delegation, commonly used as a way for Internet users to grant websites or applications access to their information on other websites but without giving them the passwords. This mechanism is used by companies such as Amazon, Google, Facebook, Microsoft and Twitter to permit the users to share information about their accounts with third party applications or websites.

Operating system: Software that manages and facilitates computer hardware and software. The operating system serves as the controlling application for the computer. Examples include Windows and Linux.

Packet: The unit by which data is communicated by computers across the internet. Packets contain the address of the originating computer as well as the destination computer.

Packet capture: Using an application programming interface to capture "packets" of information crossing a network in order to diagnose a network problem or to spot-check for malicious activity.

Passive attack: Unauthorized monitoring of system activities or interception of data without altering the system or its resources, data, or operations. Examples include traffic analysis, monitoring unencrypted communications, decrypting weakly encrypted traffic, and capturing passwords or other authentication information.

Password: A data value, usually a string of characters, that a user presents to a system to authenticate the user's identity or verify access authorization. A password is generally kept secret and paired with a user identifier, such as a user name. Authentication or verification occurs when the inputted password is matched with the password held by the access control system for the relevant user identifier.

Patch: A software modification, modification component, or the act of modifying software. A patch generally fixes a vulnerability or bug but may also enhance the software or introduce a new feature. A patch may not change the version number or release details for the related software component.

Patch management: The structured identification, notification, application, and verification of patches to installed software systems on an organization's computers.

Penetration testing: The practice of testing a system for vulnerabilities by working under specific circumstances and attempting to avoid or defeat a system's security features. Tests are either automated with software applications or performed manually.

Permission: An authorization to perform some action on the system.

Persistent data: Data stored on a local hard drive or other device that remains in storage when the device is turned off. Phishing: An attempt to illegally gather personal and/or financial information from targets by sending them a message that appears to be from a trusted source. A phishing message typically includes at least one link to a fake website, designed to mimic the website of a legitimate business and trick the target into providing information that can be used for identity theft or online financial theft.

Plaintext: Unencrypted and otherwise readable text or messages. Plaintext is the input in the encryption process and output of the decryption process.

Port: A physical port is a connection point between a computer and an external or internal device. Packets of information transmitted on the internet are separated into separate streams, or virtual ports, based on type. Each packet is assigned a number based on the port, which allows the receiving system to recognize what it is receiving. For example, secure online data is generally assigned to Port 443.

Port scan: Use of a program to identify which ports on a computer are open. A port scan will allow a user to know which ports are open to send packets to.

Privilege: Authorization to a program, person, or process to functions on a system including security-related functions.

Privileged Access Management (PAM): Cybersecurity strategies and technologies for exerting control over the elevated ("privileged") access and permissions for users, accounts, processes, and systems across an IT environment.

Privileged Identity Management (PIM): Time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access to important resources in an organization.

Protocol: A set of rules for communications that computers use when sending signals among themselves.

Proxy server: An intermediary server between an internet user and the Internet that connects users to the internet.

Public key infrastructure (PKI): The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. Framework established to issue, maintain, and revoke public key certificates.

Quality of service (QoS): The measurable end-to-end performance properties of a network service, which can be guaranteed in advance by a Service Level Agreement between a user and a service provider, so as to satisfy specific customer application requirements. Note: These properties may include throughput (bandwidth), transit delay (latency), error rates, priority, security, packet loss, packet jitter, etc.

Quarantine: Storing files that may contain malware in isolation, away from other files or other systems. The file is stored in isolation for later analysis, removal, or disinfection.

Radio frequency identification (RFID): A system that wirelessly transmits identity or other information stored in a tag using radio waves. The system consists of a transponder (the tag), an antenna, and transceiver. The antenna and transceiver are often combined into one reader. The antenna transmits a signal using radio waves that activates the transponder, which then transmits data back to the antenna.

Ransomware: A type of malware designed to lock or encrypt files on the infected computer system and display messages demanding a fee to unlock the system.

Red team: A group of white-hat, non-malicious hackers authorized to attack an organization's computer systems using the same tactics that malicious hackers would use. Instead of damaging systems or stealing information, the Red Team reports its findings to the organization to help it understand threats to its security and what measures the organization is employing work.

Redundancy: A system design in which a component is duplicated so that if it fails there will be a backup.

Remote access: The ability of a user to control a computer or device on an organization's network or the internet regardless of where the user is.

Risk assessment: The process of systematically identifying an organization's valuable resources and threats to those resources, quantifying loss exposure based on frequency of loss and cost of occurrence, and making recommendations on how to allocate available resources to defend against or mitigate loss exposure.

Risk management framework (RMF): A structured approach used to oversee and manage risk for an enterprise.

Role-based access control (RBAC): Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals.

Rootkit: A tool intruders may use to gain administrator-level access to a computer to conceal their actions and grant access to valuable data. These tools are generally difficult to detect and are installed by cracking a password or through a known vulnerability to access a remote computer.

Router: A computer-networking device that forwards data packets across a network via routing. The device acts as a junction between two or more networks transferring data packets.

Safeguards: Physical, administrative, or technical countermeasures to avoid, detect, counteract, or mitigate security risks to a computer system or network.

Scanning: Inspection of a computer or network for vulnerabilities or security holes by sending packets or requests.

Secure hash algorithm (SHA): A hash algorithm with the property that it is computationally infeasible 1) to find a message that corresponds to a given message digest, or 2) to find two different messages that produce the same message digest.

Security analytics: The study of trends, patterns, and associations in large sets of disparate data to measure its importance in managing risk and making sound decisions.

Security Assertion Markup Language (SAML): A protocol consisting of XML-based request and response message formats for exchanging security information, expressed in the form of assertions about subjects, between on-line business partners.

Security assessment report (SAR): Provides a disciplined and structured approach for documenting the findings of the assessor and the recommendations for correcting any identified vulnerabilities in the security controls**.**

Security information and event management (SIEM): Application that provides the ability to gather security data from information system components and present that data as actionable information via a single interface.

Security orchestration, automation, and response (SOAR): Designed to help security teams manage and respond to endless alarms at machine speeds. SOAR platforms take things a step further by combining comprehensive data gathering, case management, standardization, workflow and analytics to provide organizations the ability to implement sophisticated defense-in-depth capabilities.

Security requirements traceability matrix (SRTM): Matrix documenting the system's agreed upon security requirements derived from all sources, the security features' implementation details and schedule, and the resources required for assessment.

Server: System entity that manages and provides access to a resource or service within a network following requests from users or computers.

Shareable content object reference model (SCORM): A collection of standards and specifications for web-based electronic educational technology (also called e-learning). It defines communications between client side content and a host system (run-time environment), which is commonly supported by a learning management system (LMS).

Single sign-on (SSO): is an authentication scheme that allows a user to log in with a single ID and password to any of several related, yet independent, software systems.

Situational awareness: The capability to perceive different security threats and events, comprehend the meaning of an organization's cybersecurity status, and project its future status to better position security mechanisms.

Sniffing: The use of software to intercept and read all the packets of data traveling on a network. This can be done to monitor network traffic. Communications appear in clear text unless they are encrypted.

Software development lifecycle (SDLC): The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.

Spam filtering: A software process that deletes or diverts suspected spam or junk email based on criteria defined in spam filters.

Spoofing: Either receiving a communication by masquerading as the legitimate recipient or sending a communication by masquerading as the legitimate sender. “IP spoofing” refers to sending a network packet that appears to come from a source other than the actual source.

Spyware: A broad category of malicious software designed to intercept or take partial control of a computer's operation without the consent of its owner or user. Spyware is typically bundled as a hidden component of other programs that users download from the Internet. Its purpose is generally to collect information about a user, such as Internet browsing habits, login information, and payment information, and transmit it to third parties.

SQL injection: Attacks that look for web sites that pass insufficiently-processed user input to database back-ends.

Standardized information gathering (SIG): a questionnaire of third-party information security and privacy questions, indexed to multiple regulations and control frameworks.

Supply chain risk management (SCRM): A systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout the supply chain and developing mitigation strategies to combat those threats whether presented by the supplier, the supplies product and its subcomponents, or the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation, and disposal).

System (software) development life cycle (SDLC): The scope of activities associated with a system, encompassing the system’s initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal.

System integrity: The condition of a system where it is performing its intended functions without degradation or being impaired by changes or disruptions to its environments.

Tabletop exercise: An activity where personnel responsible for emergency management are gathered to discuss various simulated emergency situations.

Terabyte: One thousand gigabytes.

Third-party risk management (TPRM): Process of identifying, assessing and controlling these and other risks presented throughout the lifecycle of your relationships with third-parties.

Threat intelligence: A collection of focused information on potential threats and gaps in security based on artifacts related to threats such as associated files and communication protocols.

Token: A device that generates a random number that changes at regular intervals. This number is used, generally with a username and password, to authenticate an individual.

Traffic: Packets of information being transmitted over a network**.**

Transport layer security (TLS): Provides privacy and data integrity between two communicating applications. It is designed to encapsulate other protocols, such as HTTP. TLS v1.0 was released in 1999, providing slight modifications to SSL 3.0.

Trojan horse: A malicious computer program or application that has a seemingly legitimate function but also contains an unexpected and usually destructive function that circumvents security mechanisms. They are distinguishable from viruses because they do not replicate themselves. For a Trojan horse to spread, users must invite the program onto their computers, for example by opening an infected email attachment.

User behavior analytics (UBA): A cybersecurity process about detection of insider threats, targeted attacks, and financial fraud. UBA solutions look at patterns of human behavior, and then apply algorithms and statistical analysis to detect meaningful anomalies from those patterns—anomalies that indicate potential threats.

Verification: The process of checking the truth of an assertion by examining evidence or testing. For example, during authentication, a user's identity is verified by examining the identification information that the user presents.

Validation: The process of officially approving data structures, relationships, or systems that depend on verified items. For example, a public-key certificate is validated to confirm the relationship between an identity and a key by verifying the digital signature on the certificate.

Virus: A self-replicating computer program that executes itself and inserts copies of itself into other computer programs, data files, or the boot sector of the hard drive, thereby altering the way a computer operates. Viruses often have a harmful purpose, such as corrupting or deleting data, using the user's email program to spread itself to other computers, or taking up available hard-drive space.

Virtual private network (VPN): A means of securely accessing a private network remotely while connected to a public network. To connect to a VPN, a user first connects to the public network through an internet service provider and then uses client software on the user's device to initiate a secure connection with client software on the private network's server. Once the connection is established, the device has the same functionality, access, and security as it would if it were on the private network.

Volatile data: Data that is stored in registries, cache, and random access memory or exists in transit but is lost when a computer is no longer on.

Voice over internet protocol (VoIP): A term used to describe the transmission of packetized voice using the internet protocol (IP) and consists of both signaling and media protocols.

Vulnerability: A security flaw, glitch, or weakness in software or an operating system that can lead to security concerns. Vulnerabilities can be caused by, among other things, weak passwords, bugs in software, software misconfigurations, a computer virus or other malware, a script code injection, or an SQL injection. They exist in all software and Operating Systems and can be exploited by malicious parties.

Vulnerability assessment: The process of identifying, measuring, and prioritizing security vulnerabilities in an organization or system. Generally the assessment involves cataloging assets and resources in a system, assigning a value to those resources, identifying potential threats to each resource, and eliminating or mitigating the most serious threats to the most valuable resources.

Web Access Firewall (WAF): A specific form of application firewall that filters, monitors, and blocks HTTP traffic to and from a web service. By inspecting HTTP traffic, it can prevent attacks exploiting a web application's known vulnerabilities, such as SQL injection, cross-site scripting (XSS), file inclusion, and improper system configuration.

Web content filtering: Software that restricts or controls the content an Internet user is capable to access, especially when utilised to restrict material delivered over the Internet via the Web, e-mail, or other means. Content-control software determines what content will be available or be blocked.

White-hat hacker: A person who attempts to compromise the security of a computer system to ultimately improve its security.

Whitelist: An application whitelist is a set of administrator-approved programs that are allowed to run on a system. All other programs are blocked from running by default.

Wide area network (WAN): A physical or logical network that provides data communications to a larger number of independent users than are usually served by a local area network (LAN) and that is usually spread over a larger geographic area than that of a LAN.

Worm: A standalone malware program that self-replicates and self-propagates, spreading from system to system. Unlike a virus, a worm does not require a host file to spread. A typical result is that the worm consumes too much system memory or network bandwidth, which overwhelms servers, network servers, or individual computers.

Zero-day attack: An attack that exploits a previously unknown vulnerability in software or hardware (a “zero-day vulnerability"). “Zero day” refers to the time that elapses between when the vulnerability is made public and the first attack.

Zero trust (ZT): The main concept behind zero trust is that networked devices, such as laptops, should not be trusted by default, even if they are connected to a managed corporate network such as the corporate LAN and even if they were previously verified.

In most modern enterprise environments, corporate networks consist of many interconnected segments, cloud-based services and infrastructure, connections to remote and mobile environments, and increasingly connections to non-conventional IT, such as IoT devices. The once traditional approach of trusting devices within a notional corporate perimeter, or devices connected to it via a VPN, makes less sense in such highly diverse and distributed environments. Instead, the zero trust networking approach advocates mutual authentication, including checking the identity and integrity of devices irrespective of location, and providing access to applications and services based on the confidence of device identity and device health in combination with user authentication