Cyber Claims

Cybersecurity Glossary

In today's day and age of just about everything being stored online, the need for strong cybersecurity practices and policies has never been greater. Cybercrimes and data breaches cost companies millions of dollars every year and one slip-up in your security can dramatically impact your business's future.

While cybersecurity measures are necessary for all organizations, the conversations surrounding this topic can be difficult to understand. It is important to ensure that you and your entire workforce are educated in the field, as just one weak link in the chain can lead to a major cyber incident.

Consult this glossary to stay informed, improve upon your understanding of cybersecurity and better safeguard your company's data, finances, and future.

ACCESS—Having the ability to interact with—and possibly make alterations within—a system and its information.

ACCESS CONTROL—The process of granting or denying specific requests for or attempts to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities.

ACCESS CONTROL MECHANISM—Security measures designed to detect and deny unauthorized access and permit authorized access to an information system or a physical facility.

ACTIVE ATTACK—An intentional incursion into a system that is currently happening with the goal of altering or gaining unauthorized access to resources, data or operations. See also Passive Attack.

ACTIVE CONTENT—Software that can automatically carry out or trigger actions without the explicit intervention of a user.

This document is merely a guideline. It is not meant to be exhaustive nor be construed as legal advice. It does not address all potential compliance issues. Consult your licensed insurance representative or legal counsel to address possible compliance requirements.

ADVANCED PERSISTENT THREAT—An adversary with sophisticated expertise and significant resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical and deception).

ADVERSARY—An individual, group organization or government that intends to conduct detrimental activities.

ADWARE—Any software application that displays advertising banners while the program is running. Adware often includes code that tracks a user's personal information and passes it on to third parties without the user's authorization or knowledge. Adware can slow down your computer significantly. Over time, performance can be so degraded that a user may have trouble working productively. See also Spyware and Malware.

AIR GAP—The physical separation or isolation of a system from other systems or networks.

ALERT—A notification that a specific attack has been detected or directed at an organization's information systems.

ALLOWLIST—A list of entities considered trustworthy and granted access or privileges.

ANONYMIZERS—An anonymous proxy is a tool that attempts to make activity on the internet untraceable.

ANTISPOOFING—A technique for identifying and dropping packets that have a false source address.

ANTISPYWARE SOFTWARE—A program that specializes in detecting and blocking or removing forms of spyware.

ANTIVIRUS SOFTWARE—Software designed to detect and potentially eliminate viruses before they have had a chance to wreak havoc within the system. Antivirus software can also repair or quarantine files that have already been infected by virus activity. See also Virus and Electronic Infections.

APPLICATION—Software that performs automated functions for a user, such as word processing and the creation of spreadsheets, graphics, presentations and databases, as opposed to operating system (OS) software.

APPSEC—the process of finding, fixing and preventing security vulnerabilities at the application level, as part of the software development processes.

ASSET—A person, structure, facility, information and records, information technology systems and resources, material, process, relationships or reputation that has value.

ATTACHMENT—A file that has been added to an email—often an image or document. It could be something useful to you or something harmful to your computer. See also Virus.

This document is merely a guideline. It is not meant to be exhaustive nor be construed as legal advice. It does not address all potential compliance issues. Consult your licensed insurance representative or legal counsel to address possible compliance requirements.

ATTACK—An attempt to gain unauthorized access to system services, resources or information or an attempt to compromise system integrity.

ATTACK METHOD—The manner or technique and means an adversary may use in an assault on information or an information system.

ATTACK PATH—The steps that an adversary takes or may take to plan, prepare for and execute an attack.

ATTACK PATTERN—Similar cyber events or behaviors that may indicate an attack has occurred or is occurring, resulting in a security violation or a potential security violation.

ATTACK SIGNATURE—A characteristic or distinctive pattern that can be searched for or that can be used in matching to previously identified attacks.

ATTACK SURFACE—The set of ways in which an adversary can enter a system and potentially cause damage.

ATTACKER—An individual, group organization or government that executes an attack.

AUTHENTICATION—Confirming the correctness of the claimed identity of an individual user, machine, software component or any other entity.

AUTHENTICITY—A property achieved through cryptographic methods of being genuine and being able to be verified and trusted, resulting in confidence in the validity of a transmission, information or a message or sender of information or a message.

AUTHORIZATION—The approval, permission or empowerment for someone or something to do something.

BACKDOOR—Hidden software or hardware mechanism used to circumvent security controls.

BACKUP—File copies that are saved as protection against loss, damage or unavailability of the primary data. Saving methods include high-capacity tape, separate disk sub-systems or the internet. Off-site backup storage is ideal, sufficiently far away enough to reduce the risk of environmental damage such as from a flood, which might destroy both the primary and the backup if kept nearby.

BANDWIDTH—The capacity of a communication channel to pass data such as text, images, video, or sound through the channel in a given amount of time. Bandwidth is usually expressed in bits per second (bps).

BEHAVIOR—The extent to which an individual practices several types of cybersecurity measures to avoid or attenuate the types of cyberthreats that they are vulnerable to.

BLACKBOX—A form of testing that is performed with no knowledge of a target system's internals.

BLACKLISTING SOFTWARE—A form of filtering that blocks only websites specified as harmful. Parents and employers sometimes use such software to prevent children and employees from visiting certain websites. You can add and remove sites from the “not permitted” list. This method of filtering allows for more full use of the internet, but is less efficient at preventing access to any harmful material that is not on the list. See also Whitelisting Software.

BLENDED THREAT—A computer network attack that seeks to maximize the severity of damage and speed of contagion by combining methods—for example, using characteristics of both viruses and worms. See also Electronic Infection.

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

BLUE TEAM—A team of employees or contractors that evaluates cyberattack vulnerability and makes recommendations for improvement.

BLUEJACKING—An attack in which someone sends unsolicited messages to a Bluetooth-enabled device.

BLUESNARFING—A hacking technique in which a hacker accesses a wireless device through a Bluetooth connection.

BOT—A computer that has been compromised by a remote administrator with the intent to commit a malicious act.

BOT MASTER—The controller of a botnet that, from a remote location, provides direction to the compromised computers in the botnet.

BOTNET—A collection of computers compromised by malicious code and controlled across a network.

BRING YOUR OWN DEVICE (BYOD)—A company’s policy regarding whether employees are allowed to bring in their own devices, such as smartphones or tablets and whether those devices can then be connected to and access, company systems or networks.

BROADBAND—General term used to refer to high-speed network connections such as cable modem and Digital Subscriber Line (DSL). These types of “always on” internet connections are more susceptible to some security threats than computers that access the web via dial-up services.

BROWSER—A client software program that can retrieve and display information from servers on the World Wide Web. Often known as a “web browser” or “internet browser,” examples include Microsoft’s Internet Explorer, Google’s Chrome, Apple’s Safari and Mozilla’s Firefox.

This document is merely a guideline. It is not meant to be exhaustive nor be construed as legal advice. It does not address all potential compliance issues. Consult your licensed insurance representative or legal counsel to address possible compliance requirements.

BRUTE-FORCE ATTACK—An exhaustive password-cracking procedure that tries all possibilities, one by one. See also Dictionary Attack and Hybrid Attack.

BUG—A defect in an information system or device.

BUILD SECURITY IN—A set of principles, practices and tools to design, develop and evolve information systems and software that enhance resistance to vulnerabilities, flaws and attacks.

CAPABILITY—The means to accomplish a mission, function or objective.

CATPHISH—The fabrication of a false online identity by a cybercriminal for the purposes of deception, fraud or exploitation.

CIPHERTEXT—A translation of data into a seemingly random and unintelligible form via encryption.

CLEAR SCREEN POLICY—A policy that directs all computer users to ensure that the contents of the screen are protected from prying eyes and opportunistic breaches of confidentiality. Typically, the easiest means of compliance is to use a screen saver that engages either on request or after a specified short period of time. See also Shoulder Surfing.

CLICKJACKING—A deceptive technique in which a user is tricked into clicking a link or button without realizing it. One example of clickjacking would be a transparent webpage being loaded behind a visible page so that the target thinks that they are clicking a link on the visible page, but will actually open a potentially malicious link on the transparent one.

CLIENTSIDE—This includes what the user sees, such as text, images and the rest of the UI, along with any actions that an application performs within the user's browser.

CLOUD COMPUTING—A network that contains a pool of shared resources, data and information which can be accessed easily and quickly by those with permission.

COOKIE—A small file that is downloaded by some websites to store a packet of information on your browser. Companies and organizations use cookies to remember your login or registration identification, site preferences, pages viewed and online "shopping carts" so that the next time you visit a site, your stored information can automatically be pulled up for you. You can configure your browser to alert you whenever a cookie is being sent. You can refuse to accept all cookies or erase all cookies saved on your browser.

CONFIDENTIALITY—A property that information is not disclosed to users, processes or devices unless they have been authorized to access the information.

CONTINUITY OF OPERATIONS PLAN—A document that sets forth procedures for the continued performance of core capabilities and critical operations during any disruption or potential disruption.

This document is merely a guideline. It is not meant to be exhaustive nor be construed as legal advice. It does not address all potential compliance issues. Consult your licensed insurance representative or legal counsel to address possible compliance requirements.

CRIMEWARE—a class of malware designed specifically to automate cybercrime

CRITICAL INFRASTRUCTURE—The systems and assets, whether physical or virtual, so vital to society that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment or any combination of these matters.

CRYPTANALYSIS—The study of mathematical techniques for attempting to defeat or circumvent cryptographic techniques and/or information systems security.

CRYPTOCURRENCY—A digital currency in which transactions are verified and records maintained by a decentralized system using cryptography, rather than by a centralized authority.

CRYPTOGRAPHIC ALGORITHM—A well-defined computational procedure that takes variable inputs, including a cryptographic key and produces an output.

CRYPTOGRAPHY—The use of a mathematical process on data to ensure that it remains secure through confidentiality, authentication, integrity and non-repudiation.

CRYPTOJACKING—A type of cybercrime that involves the unauthorized use of a target's devices (computers, smartphones, tablets or even servers) by cybercriminals to mine for cryptocurrency.

CRYPTOLOGY—The mathematical science that deals with cryptanalysis and cryptography.

CRYPTOMALWARE—Malware that encrypts data on the targets device and demands a ransom to restore it.

CRYPTOMINERS—Cryptomining is an online threat that hides on a computer or mobile device and uses the machine’s resources to “mine” cryptocurrencies.

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.

CYBER EXERCISE—A planned event during which an organization simulates a cyber disruption to develop or test capabilities such as preventing, detecting, mitigating, responding to or recovering from the disruption.

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

CYBER INCIDENT RESPONSE PLAN—A set of predetermined and documented procedures to detect and respond to a cyber incident.

This document is merely a guideline. It is not meant to be exhaustive nor be construed as legal advice. It does not address all potential compliance issues. Consult your licensed insurance representative or legal counsel to address possible compliance requirements.

CYBER INFRASTRUCTURE—An electronic information and communications system and services and the information contained therein.

CYBERTHREAT INTELLIGENCE—The collecting, processing organizing and analyzing data into actionable information that relates to capabilities, opportunities, actions and intent of adversaries in the cyber domain to meet a specific requirement determined by and informing decision-makers.

CYBERATTACK— A malicious and deliberate attempt to breach the information system.

CYBERESPIONAGE—A type of cyberattack in which an unauthorized user attempts to access sensitive or classified data or intellectual property (IP) for economic gain, competitive advantage or political reasons.

CYBERSECURING—The process of hardening technologies, processes and controls to protect systems, networks, programs, devices and data from cyberattacks.

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, unauthorized use or modification or exploitation.

CYBERSECURITY ADJACENT—A number of roles that have cybersecurity responsibilities that typically form only part of their overall responsibilities within an organization.

CYBERSECURITY AWARE—Knowing what security threats are and acting responsibly to avoid potential risks.

CYBERTHREATS—Something that may or may not happen but has the potential to cause serious damage. Cyberthreats can lead to attacks on computer systems, networks and more.

CYBERWARFARE—A set of actions by a nation or organization to attack countries or institutions' computer network systems with the intention of disrupting, damaging or destroying infrastructure by computer viruses or denial-of-service attacks.

DATA AGGREGATION—The process of gathering and combining data from different sources, so that the combined data reveals new information.

DATA BREACH—An unauthorized accessing or transfer of private, usually sensitive, information.

DATA INTEGRITY—The property that data is complete, intact and trusted and has not been modified or destroyed in an unauthorized or accidental manner.

DATA LOSS—The result of unintentionally or accidentally deleting data, forgetting where it is stored or exposure to an unauthorized party.

This document is merely a guideline. It is not meant to be exhaustive nor be construed as legal advice. It does not address all potential compliance issues. Consult your licensed insurance representative or legal counsel to address possible compliance requirements.

DATA LOSS PREVENTION—A set of procedures and mechanisms to stop sensitive data from leaving a security boundary.

DATA MINING—The act of combing through large amounts of data with the goal of finding items of importance, relevance or value.

DATA THEFT—The deliberate or intentional act of stealing of information.

DATAOPS—A collaborative data management practice focused on improving the communication, integration and automation of data flows between data managers and data consumers across an organization.

DE-PERIMETERIZATION—An information security strategy to strengthens an organization's security posture by implementing multiple levels of protection, including inherently secure computer systems and protocols, high-level encryption and authentication.

DEAUTHENTICATION—To revoke the authentication of; to cause no longer to be authenticated.

DECRYPTION—The conversion of encrypted data back to its original form for the purpose of being able to understand it.

DEEPFAKE—Synthetic media that have been digitally manipulated to replace one person's likeness convincingly with that of another.

DENIAL OF SERVICE ATTACK—The prevention of authorized access to a system resource or the delaying of system operations and functions. This attack often involves a cybercriminal generating a large volume of data requests. See also Flooding.

DEVSECOPS—An approach to culture, automation and platform design that integrates security as a shared responsibility throughout the entire IT lifecycle.

DICTIONARY ATTACK—A password-cracking attack that tries all of the phrases or words in a dictionary. See also Brute-Force Attack and Hybrid Attack.

DIGITAL CERTIFICATE—The electronic equivalent of an ID card that establishes your credentials when doing business or other transactions on the web. It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures) and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

DIGITAL FORENSICS—The processes and specialized techniques for gathering, retaining and analyzing system-related data (digital evidence) for investigative purposes.

DIGITAL RIGHTS MANAGEMENT—A form of access control technology to protect and manage use of digital content or devices in accordance with the content or device provider's intentions.

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 which causes unplanned interruption in operations or functions for an unacceptable length of time.

DISRUPTIONWARE—A category of malware designed to suspend operations within a target through the compromise of the availability, integrity and confidentiality of the systems, networks and data.

DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACK—A type of cyberattack that blocks access to a resource.

DOMAIN HIJACKING—An attack in which an attacker takes over a domain by first blocking access to the domain's DNS server (see below) and then putting their own server up in its place.

DOMAIN NAME SYSTEM (DNS)—The DNS is the way that internet domain names are tracked and regulated. A website's domain name is easier to remember than its IP (internet protocol) address.

DRIVE-BY DOWNLOAD—A cyberattack that occurs automatically when a user visits a malicious, compromised or poisoned website. Drive-by downloads can install tracking tools, keystroke loggers, remote access backdoors and other malicious utilities, usually without the user noticing.

DUMPSTER DIVING—Recovering files, letters, memos, photographs, IDs, passwords, checks, account statements, credit card offers and more from garbage cans and recycling bins. This information can then be used to commit identity theft.

DYNAMIC ATTACK SURFACE—The automated, on-the-fly changes of an information system's characteristics to thwart the actions of an adversary.

ELECTRONIC INFECTIONS—Often called "viruses," these malicious programs and codes harm your computer and compromise your privacy. In addition to the traditional viruses, other common types of infections include worms and Trojan horses. Electronic infections sometimes work in tandem to do maximum damage. See also Blended Threat.

ELECTRONIC SIGNATURE—Any mark in electronic form associated with an electronic document, applied with the intent to sign the document.

ENCRYPTION—A data security technique used to protect information from unauthorized inspection or alteration. Information is encoded so that it appears as a meaningless string of letters and symbols during delivery or transmission. Upon receipt, the information is decoded using an encryption key.

EVENT—An observable occurrence in an information system or network.

EVIL TWINS—A fake wireless internet hotspot that looks like a legitimate service. When targets connect to the wireless network, a hacker can launch a spying attack on their transactions on the internet or just ask for credit card information in the standard pay-for-access deal. See also Man-in-the-Middle Attacks.

EXFILTRATION—The unauthorized transfer of information from an information system.

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 hardware or software link in a network that inspects all data packets coming and going from a computer, permitting only those that are authorized to reach the other side.

FLOODING—An attack that attempts to cause a failure in the security of a computer by providing more input, such as a large volume of data requests, than it can properly process. See also Denial of Service Attack.

FOOTPRINTING—An ethical hacking technique used to gather as much data as possible about a specific targeted computer system, infrastructure and networks to identify opportunities to penetrate them.

FUZZER—An automated software testing method that injects invalid, malformed or unexpected inputs into a system to reveal software defects and vulnerabilities.

GEOFENCING—To set up triggers so that when a device such as an internet-connected smartphone enters a defined geographical boundary, the user gets an alert.

GEOREDUNDANCY—The distribution of mission-critical components or infrastructures across multiple geographic locations.

HACKER—An individual who attempts to break into a computer without authorization.

This document is merely a guideline. It is not meant to be exhaustive nor be construed as legal advice. It does not address all potential compliance issues. Consult your licensed insurance representative or legal counsel to address possible compliance requirements.

HAZARD—A natural or man-made source or cause of harm or difficulty.

HONEYNETTING—A network set up with intentional vulnerabilities hosted on a decoy server to attract hackers.

HONEYPORT—A computer security mechanism set to detect, deflect or, in some manner, counteract attempts at unauthorized use of information.

HONEYTOKENS—A fake IT resource created and positioned in a system or network to appear to cybercriminals to be of value but is used to allow tracking and detection of hacking attempts.

HONEYPOT—A decoy used to distract would-be attackers or hackers from harming systems. Honeypots are false systems meant to look real and may contain false data. They can also be used to identify new attacks and even sometimes reveal the identity of attackers.

HTTPS—When used in the first part of a URL (i.e., https://), this term specifies the use of hypertext transfer protocol (HTTP) enhanced by a security mechanism such as Secure Socket Layer (SSL). Always look for the HTTPS on the checkout or order form page when shopping online or when logging in to a site and providing your username and password.

HYBRID ATTACK—This attack builds on other password-cracking attacks by adding numerals and symbols to dictionary words. See also Dictionary Attack and Brute-Force Attack.

ICT SUPPLY CHAIN THREAT—A man-made threat achieved by exploiting the supply chain of the information and communications technology (ICT) system, including acquisition processes.

IDENTITY ACCESS MANAGEMENT—The methods and processes used to manage subjects and their authentication and authorizations to access specific objects.

INCIDENT—An occurrence that actually or potentially results in adverse consequences to (adverse effects on) (poses a threat to) an information system or the information that the system processes, stores or transmits and that may require a response action to mitigate the consequences.

INCIDENT MANAGEMENT—The management and coordination of activities associated with an actual or potential occurrence of 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.

INDICATOR—An occurrence or sign that an incident may have occurred or may be in progress.

INDUSTRIAL CONTROL SYSTEMS—An information system used to control industrial processes such as manufacturing, product handling, production and distribution or to control infrastructure assets.

INFORMATION ASSURANCE—The policies and methods by which information and systems are protected.

INFORMATION SECURITY POLICY—An aggregate of directives, regulations, rules and practices that prescribe how an organization manages, protects and distributes information.

INFORMATION SYSTEM RESILIENCE—The ability of an information system to: (1) continue to operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (2) recover effectively in a timely manner.

INFORMATION TECHNOLOGY—Any equipment or interconnected system or subsystem of equipment that processes, transmits, receives or interchanges data or information.

INFOSEC—The processes and tools designed and deployed to protect sensitive business information from modification, disruption, destruction and inspection.

INSIDE THREAT—A person or group inside an organization that could pose a potential cyberthreat due to their knowledge of vulnerabilities within a security system.

INSTANT MESSAGING (IM)—A service that allows people to send and receive messages almost instantly. To send messages using instant messaging, you need to download an instant messaging program and know the instant messaging address of another person who use the same IM program. See also Spim.

INTEGRATED RISK MANAGEMENT—The structured approach that enables an enterprise or organization to share risk information and risk analysis and to synchronize independent yet complementary risk management strategies to unify efforts across the enterprise.

IP (INTERNET PROTOCOL) ADDRESS—A computer's inter-network address, written as a series of four 8-bit numbers separated by periods, such as 123.45.678.990. Every website has an IP Address, although finding a website is considerably easier to do when using its domain name instead. See also Domain Name System (DNS).

INTEGRITY—The property whereby information, an information system or a component of a system has not been modified or destroyed in an unauthorized manner.

INTEROPERABILITY—The ability of two or more systems or components to exchange information and to use the information that has been exchanged.

This document is merely a guideline. It is not meant to be exhaustive nor be construed as legal advice. It does not address all potential compliance issues. Consult your licensed insurance representative or legal counsel to address possible compliance requirements.

INTURUSION—An unauthorized act of bypassing the security mechanisms of a network or information system.

INTERNET SERVICE PROVIDER (ISP)—A company that provides internet access to customers.

KEYSTORES—Repositories that contain cryptographic artifacts like certificates and private keys that are used for cryptographic protocols such as TLS.

KEYSTROKE LOGGER—A specific type of electronic infection that records targets' keystrokes and sends them to an attacker. This can be done with either hardware or software. See also Trojan Horse.

LAN (LOCAL AREA NETWORK)—A connection between devices that is limited to a certain geographic area, such as a single building. Usually, all hardware, such as network cables and interconnection media, are owned and controlled by the organization using the network as opposed to a WAN (Wide Area Network), which usually uses equipment owned by a third party.

MACHINE LEARNING AND EVOLUTION—A field concerned with designing and developing artificial intelligence algorithms for automated knowledge discovery and innovation by information systems.

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 APPLET—A small application program that can be automatically downloaded and run, which then performs unauthorized functions on a system.

MALICIOUS CODE—Program code intended to perform an unauthorized function or process that will have adverse impact on the confidentiality, integrity, or availability of an information system.

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

MALVERTISING—A malicious attack that involves injecting harmful code into legitimate online advertising networks.

MALWARE—A generic term for a number of different types of malicious code. See also Adware and Spyware.

MAN-IN-THE-MIDDLE-ATTACK—Posing as an online bank or merchant, a cybercriminal allows a target to sign in over a Secure Sockets Layer (SSL) connection. The attacker then logs on to the real server, using the client's information and steals credit card numbers.

This document is merely a guideline. It is not meant to be exhaustive nor be construed as legal advice. It does not address all potential compliance issues. Consult your licensed insurance representative or legal counsel to address possible compliance requirements.

METAVERSE—A shared, immersive, persistent, 3D virtual space where humans experience life in ways they could not in the physical world.

MOVING TARGET DEFENSE—The presentation of a dynamic attack surface, increasing an adversary's work factor necessary to probe, attack or maintain a presence in a cyber target.

MULTIFACTOR AUTHENTICATION—A form of authentication that provides added security by requiring more than simply a password. The second step may include being sent a text message with a one-time code or it may be a physical feature such as a fingerprint or retina scan.

NETWORK—Two or more computer systems that are grouped together to share information, software, and hardware.

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.

OBJECT—A passive information system-related entity containing or receiving information.

OPERATING SYSTEM (OS)—Programs that manage all the basic functions and programs on a computer, such as allocating system resources, providing access and security controls, maintaining file systems, and managing communications between end users and hardware devices. Examples include Microsoft's Windows, Apple's Macintosh, and Linux.

OPERATIONAL EXCERCISE—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.

OUTSIDER THREAT—An external entity that may pose a cyberthreat to an organization.

OVERFITTING—An undesirable machine learning behavior that occurs when the machine learning model gives accurate predictions for training data but not for new data.

PASSIVE ATTACK—An intentional attack that attempts to learn or make use of information about a system, but stops short of actually trying to make any changes. See also Active Attack.

PASSWORD—A secret sequence of characters that is used as a means of authentication to confirm your identity in a computer program or online.

This document is merely a guideline. It is not meant to be exhaustive nor be construed as legal advice. It does not address all potential compliance issues. Consult your licensed insurance representative or legal counsel to address possible compliance requirements.

PASSWORD CRACKING—The process of attempting to guess passwords, given the password file information. See also Brute-Force Attacks, Dictionary Attacks and Hybrid Attacks.

PASSWORD SNIFFING—Passive wiretapping, usually on a local area network, to gain knowledge of passwords.

PATCH—A patch is a small security update released by a software manufacturer to fix bugs in existing programs. Your computer's software programs and/or operating system may be configured to check automatically for patches or you may need to periodically visit the manufacturers' websites to see if there have been any updates.

PENETRATION TESTING—An evaluation methodology whereby assessors search for vulnerabilities and attempt to circumvent the security features of a network and/or information system.

PERSONALLY IDENTIFIABLE INFORMATION—The information that permits the identity of an individual to be directly or indirectly inferred.

PHISHING—Soliciting private information from customers or members of a business, bank, or other organization in an attempt to fool them into divulging confidential personal and financial information. People are lured into sharing usernames, passwords, account information or credit card numbers, usually by clicking on a link provided. See also Vishing.

PHARMING—Redirecting visitors from a real website to a bogus one. A user enters what is believed to be a valid web address and is unknowingly redirected to an illegitimate site that steals the user's personal information. On the spoofed site, criminals may mimic real transactions and harvest private information unknowingly shared by users. With this, the attacker can then access the real website and conduct transactions using the credentials of a valid user.

PLAINTEXT—Unencrypted information.

PRECURSOR—An observable occurrence or sign that an attacker may be preparing to cause an incident.

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.

PROXYJACKING—A malicious technique where an attacker gains control over a target's proxy server, allowing them to intercept and manipulate the targets internet traffic.

PUBLIC KEY—A cryptographic key that may be widely published and is used to enable the operation of an asymmetric (public key) cryptographic algorithm.

RANSOMWARE—A type of malware that holds the target's data hostage and demands payment for the user to regain control.

RECOVERY—The process following an incident or attack with the initial goal of restoring essential, basic services and functions and a long-term goal of restoring all operations.

RED TEAM—A team authorized to simulate an attack on an organization's systems in order to test cybersecurity strength.

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.

REMOTING—A technology that allows a program to interact with the internals of another program running on a different machine.

REPOJACKING—Intentionally taking over the account of an owner or maintainer who hosts a repository.

RESILIANCE—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 particular threat will exploit a particular vulnerability, with the associated consequences.

RISK ANALYSIS—The systematic examination of the components and characteristics of risk.

RISK ASSESSMENT—The product or process which collects information and assigns values to risks for the purpose of informing priorities, developing, or comparing courses of action and informing decision making.

RISK MANAGEMENT—The process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken.

RISK-BASED DATA MANAGEMENT—A structured approach to managing risks to data and information by which an organization selects and applies appropriate security controls in compliance with policy and commensurate with the sensitivity and value of the data.

ROOTKIT—A set of software tools with administrator-level access privileges installed on an information system and designed to hide the presence of the tools, maintain the access privileges and conceal the activities conducted by the tools.

This document is merely a guideline. It is not meant to be exhaustive nor be construed as legal advice. It does not address all potential compliance issues. Consult your licensed insurance representative or legal counsel to address possible compliance requirements.

ROUTER—A hardware device that connects two or more networks and routes incoming data packets to the appropriate network. Many ISPs provide these devices to their customers and they often contain firewall protection.

SANDBOXING—A way to isolate applications, code, or operating systems to perform testing or evaluation. Actions and resources are limited during testing, allowing for evaluation without the risk of harm or damage to systems, data, or storage devices.

SCAREWARE—A cyberattack tactic that frightens people into visiting spoofed or infected websites or downloading malicious software (malware).

SCRIPT—A file containing active content (i.e., commands or instructions to be executed by the computer).

SECRET KEY—A cryptographic key that is used for both encryption and decryption, enabling the operation of a symmetric key cryptography scheme.

SECURITY AUTOMATION—The use of information technology in place of manual processes for cyber incident response and management.

SHOULDER SURFING—Looking over a person's shoulder to get confidential information. Shoulder surfing is an effective way to get information in crowded places because it is relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine or type a password. Shoulder surfing can also be done long-distance with the aid of binoculars or other vision-enhancing devices. To combat it, experts recommend that you shield paperwork or your keypad from view by using your body or cupping your hand. Also, be sure you password-protect your computer screen when you must leave it unattended and clear your desk at the end of the day. See also Clear Screen Policy.

SIGNATURE—A recognizable, distinguishing pattern.

SKIMMING—A high-tech method by which thieves capture your personal or account information from your credit card, driver's license or even passport using an electronic device called a "skimmer." Such devices can be purchased online for under $50. Your card is swiped through the skimmer and the information contained in the magnetic strip on the card is then read and stored on the device or an attached computer. Skimming is predominantly a tactic used to perpetuate credit card fraud, but is also gaining in popularity among identity thieves.

SMISHING—The fraudulent practice of sending text messages purporting to be from reputable companies in order to induce individuals to reveal personal information.

SOCIAL ENGINEERING—A euphemism for nontechnical or low-technology means such as lies, impersonation, tricks, bribes, blackmail and threats-used to attack information systems. Sometimes telemarketers and unethical employees employ such tactics.

This document is merely a guideline. It is not meant to be exhaustive nor be construed as legal advice. It does not address all potential compliance issues. Consult your licensed insurance representative or legal counsel to address possible compliance requirements.

SOCIAL NETWORKING WEBSITES—Sites specifically focused on the building and verifying of social networks for whatever purpose. There are more than 300 known social networking websites, including Facebook and LinkedIn. Such sites enable users to create online profiles, post pictures and share personal data such as their contact information, hobbies, activities and interests. The sites facilitate connecting with other users with similar interests, activities and locations. Sites vary in who may view a user's profile—some have settings which may be changed so that profiles can be viewed only by "friends."

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—Unwanted, unsolicited email from someone you don't know. Spam is often sent in an attempt to sell you something or to get you to reveal personal information.

SPIDERING—The process where hackers familiarize themselves with their targets in order to obtain credentials based on their activity.

SPEAR PHISHING—A type of social engineering aimed at people with established digital relationships such as with a bank. Spear phishing scams often look like real messages from trusted entities and will attempt to trick the target into going to a fake website and entering their credentials or personal information, such as account numbers, passwords or Social Security numbers.

SPIM—Unwanted, unsolicited instant messages from someone you don't know. Spim is often sent in an attempt to sell you something or get you to reveal personal information.

SPOOFING—Masquerading so that a trusted IP address is used instead of the true IP address. A technique used by hackers as a means of gaining access to a computer system.

SPYWARE—Software that uses your internet connection to send personally identifiable information about you to a collecting device on the internet. Spyware is often packaged with software that you download voluntarily so that, even if you remove the downloaded program later, the spyware may remain. See also Adware and Malware.

SSL (SECURE SOCKET LAYER)—An encryption system that protects the privacy of data exchanged by a website and the individual user. SSL is used by websites with URLs that begin with https instead of http.

SUPPLY CHAIN—A system of organizations, people, activities, information and resources, for creating and moving products including product components and/or services from suppliers through to their customers.

SUPPLY CHAIN RISK MANAGEMENT—The process of identifying, analyzing, and assessing supply chain risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken.

This document is merely a guideline. It is not meant to be exhaustive nor be construed as legal advice. It does not address all potential compliance issues. Consult your licensed insurance representative or legal counsel to address possible compliance requirements.

SYMMETRIC CRYPTOGRAPHY—A branch of cryptography in which a cryptographic system or algorithms use the same secret key (a shared secret key).

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.

TABLETOP EXERCISE—A discussion-based exercise where personnel meet in a classroom setting or breakout groups and are presented with a scenario to validate the content of plans, procedures, policies, cooperative agreements or other information for managing an incident.

THREAT—A circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact (create adverse consequences for) organizational operations organizational assets (including information and information systems), individuals, other organizations or society.

THREAT ACTOR—An individual, group organization or government that conducts or has the intent to conduct detrimental activities.

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 harm life, information, operations and/or property.

THREATWARE—A general term encompassing all types of malicious software on computers and electronic devices.

TICKET—Data that serves to authenticate a client’s identity and, along with a temporary encryption key, creates a credential.

TIMESTOMPING—A technique used in cybersecurity and digital forensics, where attackers modify the timestamps of files and directories on a computer system to hide their actions or impede investigations.

TROJAN HORSE—A computer program that appears to be beneficial or innocuous, but also has a hidden and potentially malicious function that evades security mechanisms. "Keystroke loggers," which record targets' keystrokes and send them to an attacker and remote-controlled "zombie computers" are examples of Trojan horses. See also Electronic Infection.

TYPOSQUATTING—A form of cybersquatting (sitting on sites under someone else's brand or copyright) that targets internet users who incorrectly type a website address into their web browser.

This document is merely a guideline. It is not meant to be exhaustive nor be construed as legal advice. It does not address all potential compliance issues. Consult your licensed insurance representative or legal counsel to address possible compliance requirements.

UNAUTHORIZED ACCESS—Any access that violates the stated security policy.

URL—An abbreviation for "Uniform (or Universal) Resource Locator." A way of specifying the location of publicly available information on the internet. Also known as a web address.

URL OBFUSCATION—Taking advantage of human error, some scammers use phishing emails to guide recipients to fraudulent sites with names very similar to established sites. They use a slight misspelling or other subtle difference in the URL, such as"monneybank.com" instead of "moneybank.com" to redirect users to share their personal information unknowingly.

VIRTUALIZATION—Creating virtual representations of servers, storage, networks and other physical machines.

VIRUS—A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting (i.e., inserting a copy of itself into and becoming part of) another program. A virus cannot run by itself; it requires that its host program be run to make the virus active. Viruses are often sent through email attachments. Also see Electronic Infection and Blended Threat.

VISHING—Soliciting private information from customers or members of a business, bank or other organization in an attempt to fool them into divulging confidential personal and financial information. People are lured into sharing usernames, passwords, account information or credit card numbers, usually by an official-looking message in an email or a pop-up advertisement that urges them to act immediately by calling the phone number provided rather than clicking on a link. See also Phishing.

VPN (VIRTUAL PRIVATE NETWORK)—A communication link between networks or systems that is usually encrypted so as to provide an isolated, private and secure means of communication.

VULNERABILITY—A flaw that allows someone to operate a computer system with authorization levels in excess of that which the system owner specifically granted.

WARDRIVING—Attackers searching for wireless networks with vulnerabilities while moving around an area in a moving vehicle.

WARGAMING—An interactive technique that immerses potential cyber incident responders in a simulated cyber scenario.

WHITELISTING SOFTWARE—A form of filtering that only allows connections to a pre-approved list of sites that are considered useful and appropriate. You can add and remove sites from the "permitted" list. This method is extremely safe but allows for only extremely limited use of the internet.

WHITE TEAM—A group responsible for refereeing an engagement between a Red Team of mock attackers and a Blue Team of actual defenders of information systems.

This document is merely a guideline. It is not meant to be exhaustive nor be construed as legal advice. It does not address all potential compliance issues. Consult your licensed insurance representative or legal counsel to address possible compliance requirements.

WORK FACTOR—An estimate of the effort or time needed by a potential adversary, with specified expertise and resources, to overcome a protective measure.

WORM—Originally an acronym for "write once, read many times," a worm is a type of electronic infection that can run independently, can propagate a complete working version of itself onto other hosts on a network and may consume computer resources destructively. Once this malicious software is on a computer, it scans the network for another machine with a specific security vulnerability. When it finds one, it exploits the weakness to copy itself to the new machine and then the worm starts replicating from there as well. See also Electronic Infection and Blended Threat.

ZOMBIE COMPUTER—A remote-access Trojan horse installs hidden code that allows your computer to be controlled remotely. Digital thieves then use robot networks of thousands of zombie computers to carry out attacks on other people and cover up their tracks. Authorities have a harder time tracing cybercriminals when they go through zombie computers.

This document is merely a guideline. It is not meant to be exhaustive nor be construed as legal advice. It does not address all potential compliance issues. Consult your licensed insurance representative or legal counsel to address possible compliance requirements.