Cyber Security Glossary

Provided by: Horst Insurance

In today’s day and age of just about everything being stored online, the need for strong cyber security practices and policies has never been greater. Cyber crimes 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 cyber security measures are necessary for all organizations, the conversations surrounding this topic can be difficult to understand. It is important to make sure 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, better your understanding of cyber security and help ensure that your company’s data, finances and future are secure.

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.

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

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.

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.

ANTI-VIRUS SOFTWARE—Software designed to detect and potentially eliminate viruses before they have had a chance to wreak havoc within the system. Anti-virus 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.

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.

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

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.

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

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).

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.

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

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

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.

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.

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.

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 victim thinks that they are clicking a link on the visible page, but will actually open a potentially malicious link on the transparent one.

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.

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

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.

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

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

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

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

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 cyber criminal generating a large volume of data requests. See also Flooding.

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.

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 cyber attack 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.

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.

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.

EVIL TWINS—A fake wireless internet hot spot that looks like a legitimate service. When victims 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.

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.

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

HTTPS—When used in the first part of a URL (e.g., 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.

HONEYPOT—A decoy used to distract would-be attackers or hackers from harming systems. Honeypots are false systems that are 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.

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.

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

INSIDE THREAT—A person or group inside an organization that could pose a potential cyber threat 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.

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).

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

KEYSTROKE LOGGER—A specific type of electronic infection that records victims' 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.

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

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 cyber criminal allows a victim 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.

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.

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.

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

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.

PASSWORD CRACKING—Password cracking is 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.

RANSOMWARE—A type of malware that holds the victim'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 cyber security strength.

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

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.

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

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.

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.

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.

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, and 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."

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.

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 victim 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.

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

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 victims' keystrokes and send them to an attacker, and remote-controlled "zombie computers" are examples of Trojan horses. See also Electronic Infection.

TWO-FACTOR 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.

URL—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.

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.

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.

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 criminals 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.