CYBERRISKS&LIABILITIES_

Cyber Security Glossary

Protecting your company from cyber risks is an ongoing, demanding task. Often, business owners feel overwhelmed when it comes to cyber security because the language used to describe operations and threats is very different from the language of the business world. Consult this glossary for clear definitions of common cyber terms.

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 authorisation or knowledge. If you gather enough of it, adware slows down your computer significantly. Over time, performance can be so degraded that you 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, 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**.

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

Authorisation: 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 on the internet. Off-site backup storage is ideal, and should be sufficiently far away to reduce the risk of environmental damage, such as floods, which might destroy both the primary and the backup if it is kept nearby.

Badware: See **Malware**, **Adware** and **Spyware**.

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. Usually expressed in bits per second.

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 maximise the severity of damage and speed of infection by combining methods—for example, using characteristics of both viruses and worms. See also **Electronic Infection**.

Blog: Short for "web log," a blog is usually defined as an online diary or journal. It is usually updated frequently and offered in a dated log format with the most recent entry at the top of the page. It often contains links to other websites along with commentary about those sites or specific subjects, such as politics, news, pop culture or computers.

Broadband: General term referring to high-speed network connections such as cable modem and Digital Subscriber Line (DSL). These types of 'always on' internet connections are actually more susceptible to some security threats than computers that access the web via dial-up service.

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 Internet Explorer, Chrome, Safari and Firefox.

Brute Force Attack: An exhaustive password-cracking procedure that tries all possibilities one by one. See also **Dictionary Attack** and **Hybrid Attack**.

Clear Desk Policy: A policy that directs all personnel to clear their desks at the end of each working day and file everything appropriately. Desks should be cleared of all documents and papers, including the contents of 'in' and 'out' trays—not simply for cleanliness, but also to ensure that sensitive papers and documents are not exposed to unauthorised persons outside of working hours.

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 confidentially. 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**.

Cookie: A small file that is downloaded by some websites to store a packet of information on your browser. Companies and organisations use cookies to remember your sign-in or registration identification, site preferences, pages viewed and online 'shopping cart' so that the next time you visit a site, your stored information can automatically be pulled up for you. A cookie is convenient but also presents potential security issues. 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.

Credit Card: A card indicating the holder has been granted a line of credit. Often sought after by criminals looking for an easy way to purchase things without having to pay for them. For this reason and others, a credit card is preferable to a debit card for online shopping since it provides a buffer between buyer and seller, affording more protections to the buyer in case there is a problem with the order or the card number is compromised. See also **Debit Card**.

Cyber Bullying: Sending or posting harmful, cruel, rude or threatening messages, or slanderous information, text or images using the internet or other digital communication devices.

Debit Card: A card linked directly to the holder's bank account, withdrawing money from the account. Not as safe as credit cards for online shopping because if problems arise, the buyer's money has already been spent and is harder to get back. See also **Credit Card**.

Denial of Service Attack (DOS): The prevention of authorised access to a system resource or the delaying of system

operations and functions. Often involves a large volume of data requests generated by a cyber criminal. 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, expiry 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.

Domain Hijacking: An attack in which an attacker takes over a domain by first blocking access to the domain's DNS server and then putting his or her own server up in its place.

Domain Name System (DNS): The way that internet domain names are located. A website's domain name is easier to remember than its Internet Protocol (IP) address.

Skipping or Dumpster Diving: Recovering files, letters, memos, photographs, IDs, passwords, cheques, account statements, credit card offers and more from rubbish 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 traditional viruses, other common infections include worms and Trojan horses. They sometimes work in tandem to do maximum damage. See also **Blended Threat**.

Encryption: A data security technique used to protect information from unauthorised 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.

End User Licence Agreement (EULA): A contract between you and your software's vendor or developer. Many times, the EULA is presented as a dialogue box that appears the first time you open the software and forces you to check 'I accept' before you can proceed. Before accepting, though, read through it and make sure you understand and are comfortable with the terms of the agreement. If the software's EULA is hard to understand or you can't find it, beware!

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 internet transactions, or just ask for credit card information in the standard pay-for-access deal. See also **Man-in-the-middle Attacks**.

File-sharing Programs: Sometimes called peer-to-peer (P2P) programs, these allow many different users to access the same file at the same time. These programs are often used to illegally upload and download music and software.

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 authorised 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**.

Grooming: Using the internet to manipulate and gain trust of a minor as a first step towards the future sexual abuse, production or exposure of that minor. Sometimes involves developing the child's sexual awareness and may take days, weeks, months or, in some cases, years to manipulate the minor.

Hacker: An individual who attempts to break into a computer without authorisation.

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

Hybrid Attack: Builds on other password-cracking attacks by adding numerals and symbols to dictionary words. See also **Dictionary Attack** and **Brute Force Attack**.

Instant Messaging (IM): A service that allows people to send and get 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 uses 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.

Malware: A generic term for a number of different types of malicious code. See also **Adware** and **Spyware**.

Man-In-the-middle Attack: An attack in which a cyber criminal poses as an online bank or merchant and allows a victim to sign in over an SSL connection. The attacker then logs onto the real server using the client's information and steals credit card numbers.

Monitoring Software: Software products that allow parents to monitor or track the websites or email messages that a child visits or reads. See also **Blacklisting Software** and **Whitelisting Software**.

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

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 Windows, Macintosh and Linux.

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: 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 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 whether there have been any updates.

Peer-to-peer (P2P) Programs: See **File-sharing Programs**.

Phishing: Soliciting private information from customers or members of a business, bank or other organisation 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, often 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 shared by users. With this, the attacker can then access the real website and conduct transactions using the credentials of a valid user.

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 protections.

Script: A file containing active content—such as commands or instructions—to be executed by the computer.

Shoulder Surfing: Looking over a person's shoulder to get confidential information. It is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as he or she fills out a form, enters a PIN number at a cashpoint or types a password. 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 with your body or by 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 Desk Policy** and **Clear Screen Policy**.

Skimming: A high-tech method by which thieves capture your personal or account information from your credit card, driving licence or even passport using an electronic device called a 'skimmer'. Your card is swiped through the skimmer and the information contained in the magnetic strip on the card is then read into and stored on the device or an attached computer. Skimming is predominantly a tactic used to perpetuate credit card fraud, but is gaining popularity amongst identity thieves.

Social Engineering: A euphemism for non-technical or low-technology means—such as lies, impersonation, tricks, bribes, blackmail and threats—used to attack information systems. Sometimes telemarketers or unethical employees employ such tactics.

Social Networking Websites: Sites specifically focused on the building and verifying of social networks. 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 who have 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'. See also **Blogs**.

Spam: Unwanted, unsolicited email from someone you don't know. Often sent in an attempt to sell you something or

get you to reveal personal information.

Spim: Unwanted, unsolicited instant messages from someone you don't know. 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 personal information about you to a collecting device on the internet. It is often packaged with software that you download voluntarily, and even if you remove the downloaded program later, the spyware may remain. See also **Adware** and **Malware**.

Secure Socket Layer (SSL): An encryption system that protects the privacy of data exchanged by a website and the individual user. Used by websites whose URLs begin with HTTPS instead of HTTP.

Trojan Horse: A computer program that appears to be beneficial or innocuous, but has a hidden and potentially malicious function that evades security mechanisms. A keystroke logger, which records victims' keystrokes and sends them to an attacker, and remote-controlled 'zombie computers' are examples of damage that can be done by Trojan horses. See also **Electronic Infection**.

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: The use of phishing emails to guide recipients to fraudulent sites with names very similar to established sites. Fraudulent sites have 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 piece of computer software, usually malicious logic, that propagates by inserting a copy of itself into and becoming part of another program. A virus cannot run by itself; to be active it requires that its host program be run. Often sent through email attachments. See also **Electronic Infection** and **Blended Threat**.

Vishing: Soliciting private information from customers or members of a business, bank or other organisation in an attempt to fool them into divulging confidential personal and financial information. People are lured into sharing user names, 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—but in a vishing scam, they are urged to call the phone number provided rather than clicking on a link. See also **Phishing**.

Vulnerability: A flaw that allows someone to operate a computer system with authorisation 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 for children. Parents sometimes use such software to prevent children from visiting all but certain websites. You can add and remove sites from the 'permitted' list. This method is safe, but allows for only extremely limited use of the internet.

Worm: Originally an acronym for 'Write once, read many times', 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 starts replicating from there, as well. See also **Electronic Infection** and **Blended Threat**.

Zombie Computer: A computer controlled remotely with hidden code installed by a remote-access Trojan horse. 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 use zombie computers.