STORM CyberDecider

Terms

Terms	Suggested Policy Terms	Benefit
Computer system	All electronic computers including operating systems, software, hardware and all communication and open system networks or websites and mobile devices including but not limited to laptops, data storage devices, smartphones, iPhones, tablets, personal digital assistants, electronic office equipment, and equipment controlling manufacturing processes, or forming part of machinery.	The benefit of this definition is the exclusions will then have to deal with parts of the computer network that insurers do not want to cover, rather than hiding exclusions in definitions which several policies do at present. NB: Some policies do not include Industrial Control Systems (ICS) within their definitions, You can use CyberDecider to identify these.
Data	Any electronically stored digital or digitised information or media.	The benefit of this definition is that it makes it clear that the term 'Data' is only applicable for digital data, and where insurers want to provide broader cover, they can add terms for non-electronic data as a separate definition. Use CyberDecider to identify policies that include information stored electronically and paper as data.
Security incident	Security Incident means unauthorised access to or use of your computer system by any person not authorised to do so, including employees; or use of your computer system by an authorised person, including employees for an unauthorised purpose.	In this case, too many existing definitions fail to make it clear whether hacking or stealing of data by employees is covered by the policy. This is important as usually policies exclude deliberate acts by the insured's senior employees (directors, and partners). CyberDecider will show if hacking by employees is covered.
Privacy breach	Privacy Breach is the actual or suspected breach of any legal, regulatory or contractual requirement to protect the security or confidentiality of any information held by the insured.	The advantage with this definition is that if insurers then want to limit this, a contractual liability or proprietary information exclusion can be used for clarity. Additionally, insurers may want to limit notification cover to breaches of Data Protection legislation only. CyberDecider will identify if non-personal data is covered.
Social Engineering	Social engineering' is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purpose, not including.	Insurers can list the methods of social engineering they do not want to cover. CyberDecider identifies if cover social engineering is included and in the comments section will highlight any limitations to the extent of social engineering cover provided, e.g. where only targeted attacks are covered.

STORM CyberDecider

Definitions

Term	Definition
Advanced Persistent Threat (APT)	A type of high-level targeted attack carried out by an attacker who has time and resources to plan an infiltration into a network. These are usually seeking to obtain information, proprietary or economic, rather than simple financial data. APTs are persistent in that the attackers may remain on a network for some time and usually bypass regular security controls.
Adware	Adware is software that displays advertisements on your computer. Adware, or advertising-supported software, displays advertising banners or pop-ups on your computer when you use an application. This is not necessarily a bad thing. However, adware becomes a problem if it installs itself on your computer without your consent or installs itself in applications other than the one it came with and displays advertising. Adware can slow down your PC or your internet connection by downloading advertisements. Sometimes programming flaws in the adware can make your computer unstable.
Air Gap	The physical separation or isolation of a system from other systems or networks.
Anti-malware/ anti-virus (AV)	Software which uses a scanner to identify programs that are or may be malicious.
Backdoor (Trojan)	A piece of malicious software which allows someone to take control of a user's computer without their permission.
Blacklist	A list of entities, IP addresses etc. that are blocked or denied privileges or access.

Term	Definition
Botnet	A botnet is a collection of infected computers that are remotely controlled by a hacker. Once a computer is infected with a 'bot', the hacker can control the computer remotely via the internet. From then on, the computer does the bidding of the hacker, although the user is completely unaware. Collectively, such computers are called a botnet. The hacker can share or sell access to control the botnet, allowing others to use it for malicious purposes. For example, a spammer can use a botnet to send out spam email. Up to 99% of all spam is now distributed in this way. This enables the spammers to avoid detection and to get around any blacklisting applied to their own servers. It can also reduce their costs because the computer's owner is paying for the internet access.
Cookie	When you visit a website, it can place a file called a cookie on your computer. This enables the website to remember your details and track your visits. Cookies can be a threat to confidentiality, but not to your data. Cookies were designed to be helpful. For example, if you submit your ID when you visit a website, a cookie can store this data, so you don't have to re-enter it the next time. Cookies do not harm your data. However, they can compromise your confidentiality. Websites gradually build up a profile of your browsing behaviour and interests. This information can be sold or shared with other sites, and advertisers.
Data Loss Prevention (DLP)	A set of procedures and software tools to stop sensitive data from leaving a network.
Domain Name System (DNS)	The phone book of the internet. It allows computers to translate website names, into IP addresses so that they can communicate with each other.

Term	Definition
DNS hijacking	An attack which changes a computer's settings to either ignore DNS or use a DNS server that is controlled by malicious hackers. The attackers can then redirect communication to fraudulent sites.
Drive-by download	A drive-by download is the infection of a computer with malware when a user visits a malicious website. Drive-by downloads occur without the knowledge of the user. Simply visiting an infected website may be sufficient for the malware to be downloaded and run on a computer. Vulnerabilities in a user's browser are exploited in order to infect them. Hackers continually attack legitimate websites in order to compromise them, injecting malicious code into their pages. Then, when a user browses that legitimate (but compromised) site, the injected code is loaded by their browser, which initiates the drive-by attack. In this manner, the hacker can infect users without having to trick them into browsing a specific site.
Encryption	The process of converting information or data into a code, so that it is un-readable by anyone or any machine that doesn't know the code.
Endpoint	An internet-capable hardware device. The term can refer to desktop computers, laptops, smart phones, tablets, printers, etc.
Firewall	A barrier between networks or parts of a network, blocking malicious traffic or preventing hacking attempts. The firewall inspects all traffic, both inbound and outbound, to see if it meets certain criteria. If it does, it is allowed; if not, the firewall blocks it.

Term	Definition
Hashing	A process that uses an irreversible encryption algorithm to turn a data entry into a random alphanumeric value. Typically used to protect passwords from compromise in the event that a malicious actor gains access to the database where they are kept. Often combined with 'salting' (see below).
Intrusion Detection System (IDS)	A device or software application that monitors a network or systems for malicious activity or policy violations, with any unusual activity being flagged.
Intrusion Prevention System (IPS)	A proactive version of IDS that can automatically take actions to block suspicious behaviour.
ISO 27001	The international standard that describes best practice when it comes to information security risk management.
Keylogger	A type of malware that can secretly record a user's keystrokes and send them to an unauthorised third party.
Malware	A general term for malicious software. Malware includes viruses, worms, Trojans and spyware. Many people use the terms malware and virus interchangeably.
NIST cybersecurity framework	A set of standards, best practices, and recommendations for improving cyber security. It is industry, geography and standards agnostic, and is outcome rather than input-focused.
Patches	Software and firmware add-ons designed to fix bugs and security vulnerabilities.

Term	Definition
Payment card industry data security standard (PCI-DSS)	A data security standard created by the Payment Card Industry Security Standards Council that governs how companies accepting payments by credit/debit card have to handle and protect that information. There are four tiers of governance, based on the volumes of transactions that a company is handling, from level 4 at the bottom end to level 1 at the top.
Penetration testing	A process whereby assessors search for vulnerabilities and attempt to circumvent the security features of a network and/or information system.
Phishing	Phishing refers to the process of tricking recipients into sharing sensitive information with an unknown third party. Typically, you receive an email that appears to come from a reputable organisation, such as a bank. The email includes what appears to be a link to the organisation's website. However, if you follow the link, you are connected to a replica of the website. Any details you enter, such as account numbers, PINs or passwords, can be stolen and used by the hackers who created the bogus site. To protect against phishing attacks, it is good practice not to click on links in email messages. Instead, you should enter the website address in the address field and then navigate to the correct page or use a bookmark or a Favourite link.
Phreaking	Also called telephone hacking, it is using a computer or other device to trick a phone system. Typically, phreaking is used to make free phone calls or to have calls charged to a different account.
Ransomware	A piece of malicious software that encrypts or blocks access to data/systems, with a decryption key only being provided upon payment of a fee.

Term	Definition
Rootkit	A rootkit is a piece of software that hides programs or processes running on a computer. It is often used to conceal computer misuse or data theft. A significant proportion of current malware installs rootkits upon infection to hide its activity. A rootkit can hide keystroke loggers or password sniffers, which capture confidential information and send it to hackers via the internet. It can also allow hackers to use the computer for illicit purposes (e.g., launching a denial-of-service attack against other computers, or sending out spam email) without the user's knowledge.
Secure File Transfer Protocol (SFTP)	A methodology for exchanging/transmitting files over the internet in an encrypted format.
Secure Sockets Layer (SSL)	A protocol for transmitting private data via the internet by utilising cryptographic systems that use two keys to encrypt data.
Security Information and Event Management (SIEM)	A security solution that provides visibility of a company's cyber security by aggregating alerts and logs generated by multiple sources and security assets (IPS, IDS, AV, etc.).
Social Engineering	Social engineering' is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purpose, not including.

Term	Definition
Spearphishing	A targeted phishing attack against a certain individual, generally by role or name.
Spoofing	When the sender address of an email is forged for the purposes of social engineering/phishing.
Spyware	Software that permits advertisers or hackers to gather sensitive information without your permission. When spyware runs on the computer, it may track your activity (e.g., visits to websites) and report it to unauthorised third parties, such as advertisers. Spyware consumes memory and processing capacity, which may slow or crash the computer.
SQL injection	SQL is a computer programming language to tell a database what to do. An SQL injection is where that language is manipulated to instruct the database to perform a different task to what was intended.
Trojan	Malicious programs that pretend to be legitimate software, but actually carry out hidden, harmful functions.
Transport layer security (TLS)	The successor to SSL - a protocol for transmitting private data via the internet by utilising cryptographic systems that use two keys to encrypt data. The presence of TLS is usually shown by showing a padlock or security certificate near the website address field.
Virtual Private Network (VPN)	A method of connecting remote computers to a central network, allowing users to communicate or access the organisation's servers securely over the internet.

Term	Definition
Virus	Malicious computer programs that can spread to other files.
Vulnerability	Bugs in software programs that hackers exploit to compromise computers.
Whitelist	A list of entities, IP addresses, applications etc. that are considered trustworthy and are granted access or privileges.
Worm	A form of malware that can replicate and spread without the need for human or system interaction. Worms differ from computer viruses because they can propagate themselves, rather than using a carrier program or file. They simply create exact copies of themselves and use communication between computers to spread. Worms are capable of spreading very rapidly, (e.g. WannaCry) infecting large numbers of machines. Some worms open a "back door" on the computer, allowing hackers to take control of it. Such computers can then be used to send spam mail.
Zombie (aka bot)	A zombie is an infected computer that is remotely controlled by a hacker. It is often part of a botnet, which is a network of many zombie, or bot, computers. Once a hacker can control the computer remotely via the internet, the computer is a zombie.
Zero-day vulnerability	A software bug, unknown to the developers, that hackers have detected and can exploit to adversely affect computer programs, data, additional computers or a network.