Cyber Jargon Explained

It is not surprising that Cyber insurance involves a lot of technical jargon. This can sometimes get in the way of understanding the insurance cover and the supporting services that come with it. Here are some straightforward explanations of some commonly used terms.

Anti-Malware/Anti-Virus protects computers and networks. Anti-Malware programmes scan the system to find, stop, and remove malware, while anti-virus software does the same for viruses. Once installed, they both work in the background, providing a real-time shield against cyber threats.

Attack Surface is the total risk an organization faces from cyber-attacks. It includes digital risks like weak passwords, physical risks like device theft or disgruntled employees, and social engineering risks like phishing attacks, texts, emails etc to trick people into giving up sensitive information.

The Cloud offers applications, data, and services that can be accessed over the internet. This means they don't need to be installed onto the network or computer system.

Cloud Service Providers offer various cloud-based services such as file storage, data back-up, and other managed IT solutions like accounting platforms to assist clients carry out their business activities.

Eradication/Forensic Cleanse is about removing any harmful elements like viruses or breaches caused by cyber-attacks on a client's network. IT experts aim to fix any damage and ensure the complete removal of threats, ensuring the environment is left secure.

Firewalls control data flow between computer systemin this way they prevent unauthorised access by intruders - especially from the internet.

Forensic Investigation involves thorough analysis by IT experts to check if a computer system or network has been tampered with. Its goal is to find any harmful files, code, or permissions inserted by attackers. It can also reveal information that has been stolen.

Malware refers to malicious software that is designed to steal data or harm computer systems. It includes viruses, spyware adware and ransomware that is often distributed through emails containing malicious links.

Multi Factor Authentication (MFA) requires users to provide different verification factors like passwords and codes to access applications or online accounts securely. E.g. you might type in your password and then receive a special code on your phone to confirm you're the authorised user.

Phishing is a common type of cyber-attack where attackers try and trick users into revealing sensitive information to steal or get into a network. Phishing tactics often include false emails or text messages disguised to look realistic to users.

Privilege Administrator Accounts have more power and capabilities than regular accounts. They can change network permissions, grant access, set up new users and install software etc. They are the "Keys to the Kingdom" and can if compromised, let cyber criminals into the network and do serious damage.

A Ransomware Event is when malicious software locks the computer system or network and all its files so they cannot be accessed. It then encrypts them so they can only be accessed with a decryption key held by the attackers, who typically demand a ransom so that the data that has been locked can be recovered.

Records contain information about individuals including past, present or future customers and employees, stored or transacted on a network. It includes personal, financial and sensitive information.

Software as a Service (SaaS) allows users to access cloud-based apps over the internet, such as email and office tools like Microsoft Office 365. It is usually purchased pay-as-you-go or as a monthly or yearly subscription from a Cloud Service Provider.

Virtual Private Network (VPN) encrypts internet traffic, protecting sensitive data and disguising your online identity. A VPN stops unauthorised people from eavesdropping on your traffic and allows you to conduct work remotely and securely.

Windows Active Directory is a Microsoft service that allows administrators to control permissions and access to network resources. Inside its database lie vital details about the system, such what users and computers there are and who's allowed to do what.

GB0512AR 0324