Cyber Acronyms

Acronym	Definition
 CISO	**Chief Information Security Officer** The executive responsible for an organisation's information and data security. Increasingly, this person aligns security goals with business enablement or digital transformation. CISOs are also increasingly in a "coaching role" helping the business manage cyber risk. Can also be known as a DPO (Data Protection Officer) or CIO.
 DDoS	**Distributed Denial of Service Attacks** Is a type of cyber attack which floods a network with fake traffic to prevent legitimate users from accessing the network. The incoming traffic flooding the victim originates from many different sources, often from thousands of hosts (such as an IoT) that have been infected with malware, which instructs the IoT to bombard the victim's website.
 DLP	**Data Loss Prevention** A DLP (system) focuses on monitoring and blocking the unauthorised movement of sensitive data. It can scan external emails and stop any such transfer that it has been set up to recognise, for example, any files that are labelled confidential or for internal-use only. It can prevent both inadvertent disclosures by employees, and malicious exfiltration of data by a hacker or malware designed to transmit data. One additional component of a DLP system is that it can be used to scan, identify, and catalogue where sensitive data is stored on the network. A DLP is particularly valuable for companies that have sensitive unstructured data, such as data stored in email or spreadsheets rather than in a more controlled database environment.
 DNS	**Domain Name System** A DNS is the phonebook of the Internet. It connects URLs (web address) with their IP address (their unique "telephone number"). For example, if you type www.travelers.co.uk into your browser, the DNS system will convert this into the correct IP address, e.g. 104.78.163.166.
 DRP/BCP	**Disaster Recovery Plan / Business Continuity Plan** A DRP and BCP provides guidance on mitigating damage and recovering from an event that impairs the assets used by a company during normal business operations. A DR or BC plan traditionally addresses events such as fire or flood, but now it is also important for companies to prepare for damage or destruction to IT systems and infrastructure.
 EDR	**Endpoint Detection & Response** Endpoint Detection & Response is a security solution that is designed to detect and respond to any suspicious activity by providing real-time monitoring. Whereas antivirus software will block malicious-looking files based on a known database, EDR will go beyond this and can protect against files that demonstrate malicious behaviour, for example, attempting to access administrative rights. Thus EDR can be critical to prevent recently-created malware from causing damage, which may not yet be included in known antivirus databases.

Acronym	Definition
 IDS	**Intrusion Detection System** A system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. An IDS provides real-time monitoring for activity that is indicative of a security compromise.
 IoT	**Internet of Things** Is the network of physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, actuators, and connectivity which enables these objects to connect and exchange data.
 IPS	**Intrusion Prevention System** An IPS is a system that monitors a network for malicious activity such as security threats or policy violations. The main function of an IPS is to identify suspicious activity, and then log information, attempt to block the activity, and then finally to report it.
 IRP	**Incident Response Plan** A written plan in place which details how a company plans to respond to a network intrusion or a data breach and is specifically designed to minimise or contain associated damage.
 MFA	**MultiFactor Authentication** An authentication tool that combines “something you know” (such as a password), “something you have” (such as a text message), and “something you are” (such as a fingerprint scan) to create a stronger access control than only requiring a password. MFA can prevent intruders from spreading across a network from a single compromised computer.
 PCI-DSS	**The Payment Card Industry Data Security Standard** An information security standard for organisations that handle branded credit cards from the major card schemes. Breaches of the standard can lead to significant contractual monetary fines and penalties.
 PII	**Personally Identifiable Information** Any data that could potentially be used to identify a data subject. Examples include a full name, email address, national insurance number, driver’s license number, bank account number, passport number etc.
 SSO	**Single Sign-On** A system which enables users to securely authenticate themselves with multiple applications and websites by logging in with a single set of credentials.
 VPN	**Virtual Private Network** A virtual private network is a specific way of providing remote access to a company’s network, in which encryption is used to provide a secure communication channel between the remote device and the network. Use of a VPN protects, for example, against eavesdropping when the remote device is using a public wi-fi access point.

TRAVELERS