

# ABCs of Cybersecurity

## 32 Cybersecurity acronyms and terms you need to know

### THREATS

Advanced Persistent Threat (APT)	Bring Your Own Device (BYOD)	Data Incident (or data breach)	Distributed Denial of Service (DDoS)
A cyber attack in which an advanced (possibly state backed) hacker or bad actor targets a specific organisation for a long period of time by staying hidden in a network.	A policy allowing employees to use personal devices to access company resources.	An event that occurs when information is accessed and/or exfiltrated by an unauthorised person or entity, like a hacker, without the knowledge of the organisation from which it came.	A type of attack in which a network is flooded with traffic from multiple sources to overload it and cause a service disruption.
Encryption	Hacker	Living off the Land	Malware
The process of converting plaintext into ciphertext using a secret key.	Also known as a bad actor or threat actor. An individual who uses a computer system to gain unauthorised access to an account or system for data.	A cybersecurity attack that involves hackers using the targets existing and known hardware and/or software resources to engage in malicious activity.	Also known as malicious software that is designed to cause harm to a computer system or network.
Phishing	Ransomware	Risk Assessment	Zero-day attack
The most common form of cybercrime in which a hacker or bad actor attempts to gain access to personal and/or company data. Phishing typically occurs via email with links containing malware.	A form of malware where bad actors encrypt information on a computer system so users are unable to access their own data and demand payment in exchange for giving back the information.	A big-picture snapshot of your current cyber risk exposure – revealing vulnerabilities and uncovering opportunities to improve defences.	A cyber-attack that infiltrates information systems through previously unknown vulnerabilities in software and/or firmware. When a company updates any server, device, or system, there is a risk of potential incidents in vulnerable areas within the update.

### SOLUTIONS

Anti-virus (AV)	Business Continuity and Disaster Recovery (BCDR)	Cloud Computing	Cybersecurity Insurance
Software used to identify and isolate (quarantine) viruses, worms, and other malicious software from endpoints (laptop, servers, mobile devices, etc.)	A solution to reduce business downtime, mitigate legal ramifications, and save SMBs from losing money as the result of disasters, whether natural or human-made.	The delivery of computing services, including servers, storage, databases, and software, over the internet.	A form of insurance that protects businesses and individuals from financial loss from cyber attacks or incidents.
Disaster Recovery Plan	Endpoint Detection and Response (EDR)	eXtended Detection Response (XDR)	Firewall
A documented procedure for an organisation to follow to recover from a disaster that impacts normal operations.	A tool that identifies and investigates threats to a business's endpoints. EDR solutions replace traditional Anti-virus software by offering more security.	An advanced security technology that combines multiple security tools and data sources to provide a more thorough and comprehensive look inside your organisation's security posture.	A network security system that monitors and controls incoming and outgoing network traffic based on security rules.
Incident Response (IR)	Managed Detection Response (MDR)	Multi-factor Authentication (MFA)	Secure Access Service Edge (SASE)
A formal, documented, and organised approach to managing the effects of a security incident or cyberattack.	A cybersecurity solution that uses EDR monitored 24/7/365 using trained expert humans (SOC) to provide a more complete cybersecurity defence.	A security method used to add a second layer of authentication when accessing accounts and/or devices. In addition to a username and password, MFA also requires codes, biometrics, or other information to sign into an account.	A cloud based zerotrust architecture which requires no onpremise hardware.
Security Information and Event Management (SIEM)	Single Sign-On (SSO)	Virtual Private Network (VPN)	Vulnerability Management
A log monitoring and archiving tool that provides your business with the ability to identify threats and anomalies in real time, or to investigate historic network, system, and user activities.	A technology that gives users access to multiple accounts with just one set of login credentials. SSO simplifies the login process and reduces the risk of poor password hygiene, like weak or reused passwords.	A remote connection method used to obfuscate all network traffic using strong encryption. VPN is often used to access a corporate network, or add security and privacy when using public networks such as in airports or hotels.	A service that routinely scans for and patches weak points in your system that could be exploited. The process provides realtime visibility into potential flaws so they can be prioritised and addressed before they pose a serious risk.

### PEOPLE

Chief Information Security Officer (CISO)	Managed Security Services Provider (MSSP)	Network Operations Centre (NOC)	Security Operations Centre (SOC)
A senior-level executive who is responsible for managing the security of a company's information and technology.	An MSP (Managed Services Provider) with a focus on security. MSSPs provide services like cybersecurity, BCDR, network monitoring, and more.	A centralised location where a team of IT professionals monitor and manage the performance and security of remote monitoring and management software.	A 24/7/365 operation staffed by expert humans who review incoming security alerts and takes immediate action to isolate and remediate potential threats before they can cause significant damage.

Get in touch today!

[Security@trustsystems.co.uk](mailto:Security@trustsystems.co.uk)