Cyber Glossary – Top 100 Terms (Clean Build, Batch 1 of 5)

Term	Definition	Genre
Access Control	Limiting who can view or use resources in a system. Like having a keycard to enter only the rooms you're allowed in.	Governance
Asset	Anything valuable to your organisation — like data, hardware, or software — that needs protection.	Governance
Attack Surface	All the points where an attacker could try to get into your systems — like doors and windows on a house.	Risk
Authentication	Proving someone is who they say they are before giving access — like showing ID at a secure building.	Technical
Authorisation	Granting access to a system or file only after someone has been verified.	Technical
Backup	A copy of important data kept safe in case the original is lost or damaged.	Response
Botnet	A group of hijacked devices used together to launch attacks — usually without the owner's knowledge.	Threats
Breach Notification	The legal or ethical requirement to inform people when their data has been exposed.	Policy
Clickjacking	Tricking someone into clicking something malicious by hiding it under a legitimate-looking page or button.	Threats
Cloud Security	Protecting data and systems stored in the cloud (off-site servers) rather than on physical devices.	Risk
Configuration	The way software or hardware is set up — incorrect settings can leave systems vulnerable.	Technical
Credentials	A user's login details — usually a username and password — that grant access to systems or data.	Data
Cyber Hygiene	Basic best practices for staying safe online — like using strong passwords and keeping software up to date.	Governance
Cyber Risk	The potential for loss or harm due to a cyber attack, system failure, or human error.	Risk
Cyber Threat	Anything that could cause harm in the digital world — from hackers to faulty software.	Threats
Cybersecurity	The practice of protecting systems, networks, and data from digital attacks or unauthorised access. Like locking the doors to your digital office.	Governance

Data Breach	When sensitive or confidential information is accessed, copied, or shared without permission.	Threats
Data Classification	Labelling information based on how sensitive or important it is — like 'public', 'internal', or 'confidential'.	Data
Data Governance	The overall management of how data is used, protected, and shared across an organisation.	Governance
Data Integrity	Making sure data is accurate and hasn't been tampered with.	Data
Data Loss Prevention (DLP)	Tools and policies that help stop sensitive data from leaving your organisation by mistake.	Data
Denial of Service Attack	An attempt to overload a system (like a website) so it becomes unusable.	Threats
Digital Footprint	The trail of data you leave behind when using the internet — including logins, posts, and browsing history.	Risk
Distributed Denial of Service (DDoS)	A large-scale DoS attack using many systems to flood and disable a service.	Threats
Domain Name System (DNS)	A system that matches website names (like google.com) to their real location online.	Technical
Endpoint	Any device connected to a network — like a phone, laptop, or printer — and a common target for cyber attacks.	Technical
Encryption	The process of scrambling data so only authorised people can read it — like sealing a letter in a locked envelope.	Data
Ethical Hacker	A person who tests systems for weaknesses so they can be fixed before bad actors exploit them.	Response
Exposure	A situation where your systems or data are at risk of being attacked or leaked.	Risk
Exploit	A method or tool used to take advantage of a weakness in a system.	Threats
Firewall	A digital barrier that blocks unwanted access to your network, like a security guard checking who's allowed in.	Technical
Framework	A structured approach for managing cyber risks, policies, and controls. Often used by boards and auditors.	Governance
Gateway	A network point that connects your organisation to the internet. If left unprotected, it can be a weak link.	Technical
Governance Framework	The set of rules and responsibilities that define how cyber risks are managed at the executive and board level.	Governance

Honeypot	A decoy system used to lure cyber attackers and study how they operate.	Response
Identity Theft	When someone steals your personal information to commit fraud.	Threats
Incident Response Plan	A formal plan for what to do when a cyber incident occurs — helps teams act fast and minimise damage.	Response
Information Asset	Any data, document, or system that has value to your organisation.	Data
Insider Threat	A risk from someone within your organisation — either accidentally or deliberately causing harm.	Threats
Intrusion Detection System (IDS)	A system that monitors network traffic for suspicious activity.	Technical
ISO 27001	A global standard for managing information security within an organisation.	Governance
Least Privilege	A policy that gives users only the access they absolutely need — nothing more.	Governance
Log / Logging	The automatic recording of events on a system, used for troubleshooting and investigations.	Technical
Machine Learning	A form of AI that helps systems spot patterns, such as detecting unusual login behaviour.	Technical
Malware	Malicious software meant to cause harm — includes viruses, spyware, ransomware, etc.	Technical
Malware-as-a-Service (MaaS)	A business model where cybercriminals rent out malware tools to others, making it easy for less skilled attackers to launch attacks.	Threats
Man-in-the-Middle Attack	When an attacker secretly intercepts and possibly alters communication between two parties.	Threats
Mobile Device Management (MDM)	Software used by organisations to control and secure employees' smartphones and tablets.	Governance
Multi-Factor Authentication	An extra layer of security requiring more than just a password to log in — like a code sent to your phone.	Risk
Network	A group of connected computers or devices that share resources and information.	Technical
Network Segmentation	Dividing a network into smaller parts to contain breaches and reduce risk.	Technical
Password Manager	A secure tool that stores and remembers complex passwords for you.	Technical
Penetration Testing	A simulated cyber attack used to test how well your systems can withstand real threats.	Response
Personally Identifiable Information (PII)	Any information that can identify a person — like names, addresses, or Medicare numbers.	Data

Phishing	A fake message (often email or SMS) designed to trick someone into giving up personal info or clicking on a harmful link.	Threats
Phishing Simulation	A controlled test to see who in your organisation might fall for a phishing attempt, used for training.	Response
Proxy Server	A server that sits between your device and the internet to filter requests and improve privacy.	Technical
Recovery Plan	A step-by-step guide to restoring operations after a cyber incident or disaster.	Response
Red Team	A group that mimics real attackers to test your organisation's defences.	Response
Risk Appetite	The level of cyber risk an organisation is willing to accept in pursuit of its goals.	Governance
Risk Register	A living document listing potential cyber risks and what's being done to manage them.	Governance
Root Cause Analysis	Investigating what led to a cyber issue so it can be fixed properly.	Response
Sandbox	A secure environment used to safely run or test suspicious software.	Technical
Scam	A fraudulent attempt to trick someone, often for money or information.	Threats
Secure Coding	Writing software in a way that avoids common security problems.	Technical
Security Operations Centre (SOC)	A team that monitors, detects, and responds to cyber threats 24/7.	Governance
Shadow IT	Hardware or software used without the knowledge or approval of IT — often risky.	Risk
Shoulder Surfing	Stealing information by watching someone type in their password or PIN.	Threats
Smishing	A type of phishing that uses SMS messages to trick people into clicking links or giving away information.	Threats
Social Engineering	Tricking people (not computers) into revealing information or doing something risky.	Threats
Social Media Threat	A risk that comes from sharing too much on platforms like Facebook or LinkedIn — attackers may use this info.	Threats
Software-as-a-Service (SaaS)	Applications delivered over the internet, like Google Workspace or Xero — convenient but needs proper access control.	Technical
Spam	Unwanted or irrelevant messages, usually sent in bulk — can be harmless or carry threats.	Threats
Spoofing	Faking a trusted identity — like an email that looks like it's from your CEO — to trick people.	Threats

Spyware	Malicious software designed to secretly watch what you do and collect information.	Threats
Supply Chain Attack	Targeting a vendor or third party to compromise your organisation indirectly.	Risk
Threat Actor	An individual or group behind a cyber attack — could be criminals, hacktivists, or state-based operatives.	Threats
Threat Intelligence	Information about current cyber threats, used to help anticipate and prevent attacks.	Governance
Two-Factor Authentication (2FA)	A security measure requiring two pieces of evidence to log in, like a password and a code.	Risk
Typosquatting	Creating a fake website with a slightly misspelled name (e.g., goggle.com) to trick users.	Threats
Unpatched Software	Programs with known vulnerabilities that haven't been fixed — a common way attackers get in.	Risk
User Awareness Training	Educating staff on how to spot and respond to cyber threats.	Governance
Virtual Machine	A software-based computer that runs within a real one — used for testing or isolating threats.	Technical
Virtual Private Network (VPN)	A secure, encrypted connection used to protect data when accessing the internet remotely.	Technical
Vulnerability	A weakness in a system that could be exploited to cause harm.	Risk
Watering Hole Attack	Compromising a site that's frequently visited by a target group — like baiting a known drinking spot.	Threats
Web Application Firewall (WAF)	A tool that protects websites by filtering out malicious traffic.	Technical
Whaling	A phishing scam that targets senior executives — big fish with big consequences.	Threats
White Hat	A friendly hacker who helps organisations find and fix security issues.	Response
Zero Trust	A security model that assumes nothing inside or outside the network is automatically trustworthy.	Governance
Zero-Day Vulnerability	A flaw in software that's unknown to the vendor and can be exploited immediately by attackers.	Risk