**Cyber Security Definitions**

**Adjustment** is about finding a way of doing things differently than normally to make it easier or harder

**Adequate** means acceptable or good enough for the situation

**Application Whitelisting** is about protecting harmful files from folders to internet from your organisation.

**Baseline** is a starting point minimum for organisations

**Bypass** is a shortcut to avoid something. In this case, bypassing passwords can cause hackers to steal passwords.

**Compromise** is the disclosure of information to people who do not have authorised access and is a violation of the security policy of a system, whether intentional or unintentionally

**Confidential** means the information shared should be kept privately or secret and not shared with anyone else

**Consequences** in this context means a bad outcome of an action/situation done by hacker

**Corporate** is a large organisation that employs at least over 1000 people and often has offices worldwide

**Cybercrime** is about computer networks and computers being hacked, copyrighted, doxing, fraud etc. usually for financial or obtaining top level clearance secrets gain.

**Data leak** is about unauthorised confidential information given to people not involved in the work projects.

**Digital Attacks** means any malicious attempt to gain unauthorized access to a computer, computing system or computer network with the intent to cause damage

0dbe698da2f08e7a1340331c02382cbe.png**Disabled** in this context means turned off completely so hackers can have no control of the computer for their target needs

**Domain administrators** are privileged user accounts for certain people e.g. IT Help Desk Recovery team

**Disaster recovery** is a set of policies, tools and procedures in place to recover or the continuation of vital technology infrastructure and systems; in any natural or human induced disaster. Disaster recovery focuses on the critical IT business functions.

**Data recovery** is about having a backup of your data in the case of a disaster (mother nature, hackers etc), so that important files are not completely lost, corrupted or made inaccessible in any technology form. The most common way to backup corporate data is on encrypted USB sticks, but not limited to that only.

**Data availability** means enterprises ensures all business related data is available to the organisation, partners, or end-users at any time whenever and wherever required.

**Detection** in this context refers to finding vulnerabilities and threats in organisations devices.

**Ethically wrong** means not morally right or not following a set of rules or procedures in place. For example, hackers target companies for financial gain is the wrong thing to do.

**Framework** in this context refers to a set of documents to describe structure, guidelines, standards or best practices for cybersecurity risk management. For example, Essential 8 or Agile Methodology. These methods exist to lessen the extent of weaknesses and vulnerabilities of organisations which hackers could exploit.

**Hackers** are people who try to get into an organisation’s computer using specialised computer software such as Trojan horse programs, computer viruses and worms which harms other people’s devices. When this threat or damage happens, this is called malware.

0dbe698da2f08e7a1340331c02382cbe.png**Identity Access Management (IAM)** is a is a framework of business processes, policies and technologies which stores the management of electronic or digital identities in a safe place. With this, information technology managers can control user access to critical information within their organizations. Examples of systems used for IAM include single sign-on systems, two-factor authentication (2FA), multifactor authentication and privileged access management. These technologies also provide the ability to securely store identity and profile data as well as data governance functions to ensure that only data that is necessary and relevant is shared so hackers are unable to get in.

**Implementation** is the [act](https://dictionary.cambridge.org/dictionary/english/act) of putting a [plan](https://dictionary.cambridge.org/dictionary/english/plan) into [action](https://dictionary.cambridge.org/dictionary/english/action) in place such as the Essential 8 framework to have this working in place

**Key Performance Indicator (KPI)** is about how the business targets and objectives are meeting the demands required for the company’s success. Whether it’s sales, marketing, customer service, or production etc., KPIs provide tangible data that indicates how well these areas are performing. This is also useful for tracking progress toward specific objectives and essentially finding smaller and measurable components to work on.

**Malicious code** refers to software that attempts to ruin the confidentiality, integrity or availability (CIA Triad) of a system.

**Malware** stands for **malicious software**, and is a bad software which can be programmed on a computer without approval from the computer owner or organisation. Malware has many forms of harming devices such as computers, laptops, phones using spyware, viruses and Trojan horses. Malware infected devices are capable of stealing passwords, erasing or modifying files, collecting personal information or even freeze the device. To reduce the risk of this, there is anti-malware software to protect the devices and users.

**Maturity** in this context refers to your organization's ability level to combat cybersecurity threats within and beyond the organisation with their technology.

**Maturity Model** is about having a sequence of discrete maturity levels for a class of processes in one or more business domains, and represents a desired outcome for the organisation.

0dbe698da2f08e7a1340331c02382cbe.png**Mechanism** in this context refers to machine parts, or a set of [parts](https://dictionary.cambridge.org/dictionary/english/part) that [work](https://dictionary.cambridge.org/dictionary/english/work) together

**Mitigation** is about reducing the risk or effect of a cyber attack threat and any vulnerabilities; from a decision, action or practice.

**Minimise** in this context is about reducing the number of cyberattack threats so does not affect devices too much

**Operations** can mean two different things in this context. **Operation** is about how a machine and system work together or the process of making this. However, operation in the cybersecurity context means a set of guidelines given [achieve](https://dictionary.cambridge.org/dictionary/english/achieve) a result of greater security controls such as the Essential 8.

**Prevention** in this context is about keeping threat actors and hackers away from confidential files

**Privileged user** is a user who has access to the other organisation’s devices and user information that modify or make changes in the system’s security measures. The capabilities can be for system configurations, account privileges, audit logs, data files or applications. Often, software developers and cybersecurity staff members have limited user privileges.

**Protect** in this scenario is about restricting the access to or use of data.

**Risk mitigation** refers to the process of understanding risks and threats and accepting that they exist but take the appropriate measures to reduce the threats - in case they happen. This is part of the risk management process to have the organization prepared for any threats to its operations and processes.

**Security Mechanism** is a mechanism that is designed to detect, prevent or recover from a cybersecurity attack

**Sensitive information** is any information that should be protected from the public including personal details like names, addresses, social security numbers, and medical records. If this information was identified, this could harm individuals or organisations due to the confidential nature.

0dbe698da2f08e7a1340331c02382cbe.png

**Threats in cybersecurity** is being in a situation which can have a negative outcome or consequence for the business operation, function, brand, reputation, or perceived image. Threats like this include the limitation of [data access](https://www.hpe.com/au/en/what-is/data-access.html), integrity, and value, as well as the people, processes, and technologies involved in managing that data. Cyber threats typically arise when an individual or organization's data, computer system, network, or device is targeted by a cyber attacker who seeks to gain unauthorized access or exploit any vulnerabilities present in the information system, compromising its confidentiality, integrity, or availability.

0dbe698da2f08e7a1340331c02382cbe.png