The Essential 8
In Plain English

CYBERGUYS

Introduction

In today's digital and interconnected world all organisations, regardless of their industry or size, are becoming more cyber security aware. But without a large team of experts to guide them, how do they know if they're doing the right things, and how do they know if they're doing them well enough?

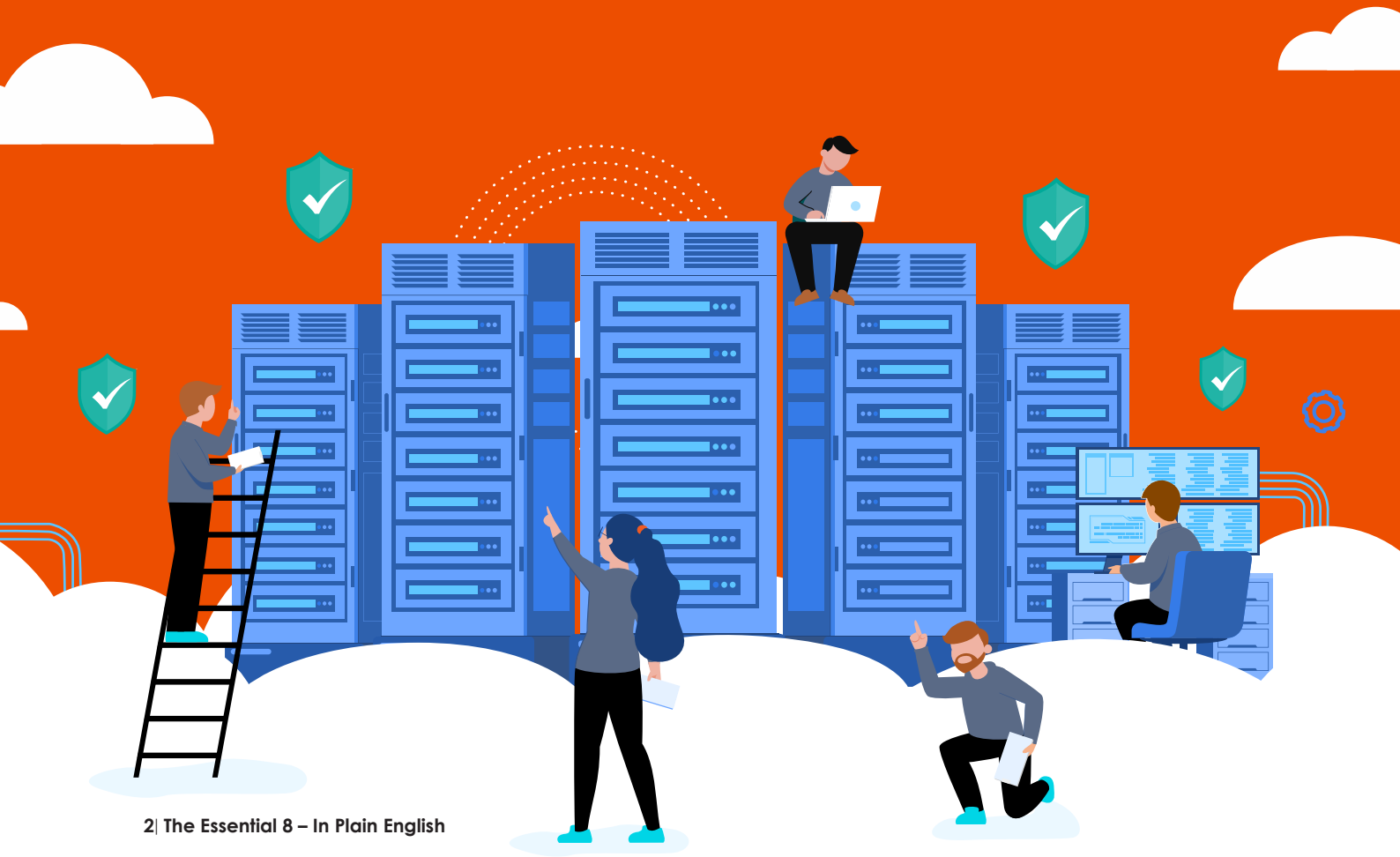
To help answer these questions, the Australian Government has produced a framework called the Essential 8 which organisations can use to identify, implement, and mature their cyber security and cyber defence strategy.

Since the Essential 8 was introduced, there has been a growing trend to use it not only to improve organisations' cyber security, but also to evidence cyber security maturity externally. The Essential 8 already form the basis of mandatory cyber security requirements for all 98 non-corporate Commonwealth entities, and various state and federal government policies have been implemented to enforce regular assessment, adherence reporting, and minimum achievement standards against the Essential 8 for suppliers within the public sector.

Such a level of supply chain transparency is also becoming more commonplace in the private sector, with more and more B2B procurement processes taking into account cyber security maturity and following the government's lead in using the Essential 8 as a reference point with which to measure it.

Whether to improve their own cyber defences, to become eligible for public-sector procurement or to become more competitive in private-sector procurement, business leaders need an understanding of the Essential 8 as it is quickly becoming the de facto standard for measuring and evidencing cyber security in Australia.

This paper explains the Essential 8 framework in plain English so business leaders from all background can gain a working knowledge of how these cyber strategies and maturity criteria can be used to improve defences and gain advantage over competitors.



What is the Essential 8?

The Essential 8 is a cyber security framework produced by Australian Cyber Security Centre (ACSC) which contains eight cyber defensives strategies, and four maturity levels to which each strategy can be implemented.

The ACSC actually recommends thirty-seven defensive strategies each of which is given an effectiveness rating ranging from 'limited' to 'essential'. The formal scope of the Essential 8 framework, however, only includes the eight strategies rated as 'essential', and only provides maturity criteria for these strategies.

The framework is intended to help organisations baseline and measure their current cyber security practice, as well as provide industry-aligned targets which can be used to identify areas of improvement to achieve greater cyber security maturity.

Eight Essential Mitigation Strategies

The eight mitigation strategies that the ACSC rates as essential for all organisations are:

1. **Application control** – Considers how and where different types of executable files (applications) are allowed to run. Essentially, this strategy seeks to ensure that programs cannot be installed and run without correct authorisation. It prevents users from installing new and unknown software from the internet, and stops malware from installing and running itself.

2. **Patch applications** – Looks at how quickly patches from software vendors are installed, as well as how the organisation identifies missing patches. Software patches often target time-sensitive vulnerabilities, so by quickly installing these fixes and using scanning tools to ensure all devices are up to date, organisations can prevent cyber criminals from using known gaps within a product to penetrate the corporate environment.

3. **Configure Microsoft Office macro settings** – Office macros are small programs that can run automatically inside of a Word, Excel or PowerPoint document when opened. They have been an entry point for malware for many years now; this strategy seeks to ensure Office macros are only enabled when absolutely necessary, and users are not allowed to alter their own Office macro settings.

4. **User application hardening** – Looks at the configuration of user applications, with specific focus on web browsers and Microsoft Office. It ensures common entry points for malware, such as Java and web advertising, are blocked, and prevents users from modifying applications' security configurations.

5. **Restrict administrative privileges** – Ensures that users who do not require the ability to administer systems are not given it, as well as enforces strict controls on users who do administer systems. Most malware requires some level of administrative access in order to function, so by limiting these privileges to only those who need them, organisations can greatly reduce their cyber risk.

6. **Patch operating systems** – This strategy is similar to application patching but focuses on the operating system (Windows). Microsoft releases patches and updates on a regular schedule; rapid patching is critical as cyber criminals rush to exploit known vulnerabilities in Windows due to its massive user base.

7. **Multi-factor authentication** – Includes a variety of additional authentication methods, such as one-time passcodes and smart phone authentication apps. These measures make stealing passwords and taking over accounts much harder, and greatly reduce an organisation's risk profile.

8. **Regular backups** – Backups form a key recovery strategy for cyber incidents. If data is lost, destroyed, or encrypted for ransom, recovering from a recent backup can be a quick, simple, and effective means of averting a crisis. Having backups in place and aligned to organisational data requirements is an important risk mitigation strategy.

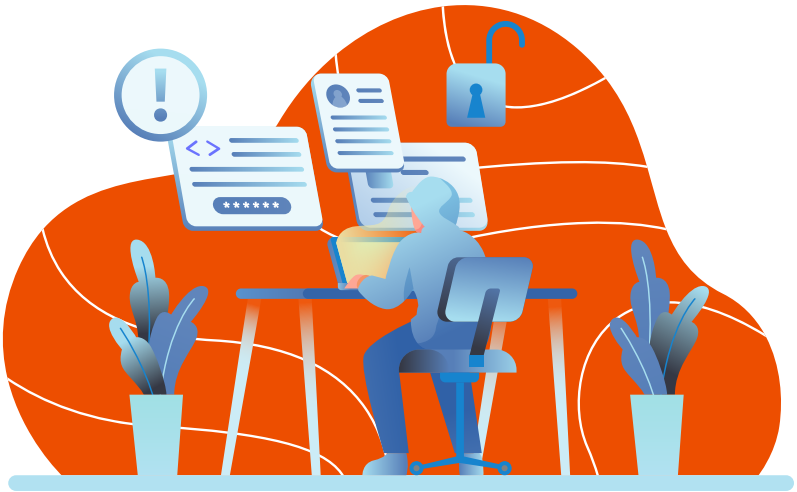
Four Maturity Levels

The Maturity Model of the Essential 8 includes four separate maturity definitions. Each maturity level represents protection against increasingly sophisticated 'tradecraft', or capability, of a potential cyber adversary, and each is defined by increasingly strict criteria.

In essence, if an organisation is comfortable only protecting itself from the most basic cyber crime techniques, it may choose maturity level one. If, however, the organisation wishes to protect itself from moderately skilled cybercriminals who are willing to invest time into an attack, it should target maturity level two. Maturity level three is for organisations who need to protect against more determined adversaries who may target an attack to that organisation's specific defences and weaknesses.

To take strategy 2, patching of applications, as an example, to achieve level one maturity an organisation must install patches within one month of the vendor releasing them. Level two maturity requires installation with two weeks of release, and level three also requires patching within two weeks, however adds the requirement for installing patches with known exploits within forty-eight hours.

In choosing a target maturity level, organisations should consider their own desirability to cyber criminals, as well as the impact a cyber incident would have on their business. This consideration, along with the descriptions of each maturity level below, can be used to help determine a target maturity level for an organisation to implement.



Maturity Level Zero – A classification given to organisations that have not implemented the basic maturity in the essential mitigation strategies. Organisations falling into this category are exposed and vulnerable to loss, outage and other impacts associated with a cyber incident. A cyber incident could be perpetrated by even the most basic of adversaries.

We would not recommend this maturity level for any organisation, as it represents fundamental security measures not being in place. While an organisation at this maturity level may survive for a period of time without a cyber attack, they are only safe because no one has yet attempted an attack.

To use an analogy, an organisation at this level of maturity is similar to a car which is left each night with its doors and windows open. While the car may last a while with nothing stolen from inside, even a basic glance by anyone walking past reveals the lack of security. Theft of items is only prevented by the morals of those walking by.

Maturity Level One – This maturity level caters to organisations looking to mitigate attacks by adversaries with limited experience and capability.

These adversaries will usually have only rudimentary knowledge of cyber crime tradecraft, relying on publicly available scripts and exploits to carry out simple attacks wherever they can find an exposed victim. They rarely target specific organisations, instead settling on any victim with defences weak enough for them to penetrate.

We recommend this maturity level only for new micro-businesses with no other risk factors which make them desirable to cyber criminals. At this maturity level an organisation is resistant to cyber criminals scanning the internet for obvious weaknesses, but its defences are unlikely to hold up in the face of a determined and capable attacker.

To continue the analogy, the car would be left each night with doors and windows closed, but not locked. Opportunistic criminals passing by would be unlikely to identify weaknesses; however, a thief with even a slight degree of determination, such as those testing all the car door handles in the local area, will easily be able to break into the car.

Maturity Level Two – The focus of this maturity level is adversaries with a moderate degree of knowledge. While these adversaries still lack advanced cyber attack tradecraft, they are likely to employ phishing and social engineering to steal credentials as well as purchase 'cyber crime as a service' toolkits to fill their own capability gaps. These kits are used to deploy malware and ransomware developed by more sophisticated cyber criminals.

Adversaries at this maturity level are likely to invest more time into targeting each organisation but will still be conservative with their efforts and likely target multiple organisations at once.

We recommend this maturity level for SMEs without any additional factors which make them desirable to cyber criminals.

In our car analogy, an organisation at maturity level two is like a car which has its windows and doors closed and locked each night. Most opportunistic crime is prevented, and gaining illegal entry requires specific tools and targeting that is beyond all but the most determined of thieves.

Maturity Level Three – The ACSC's highest maturity level aims to protect against adversaries with highly developed tradecraft who adapt their attacks to each new target. These adversaries have a library of capabilities at their disposal, and they take the time to assess each organisation they target for its particular weaknesses and then design ways to circumvent them. Once they have penetrated defences, they can pivot and use other techniques to maximise the damage they cause, or the value they extract.

We recommend SMEs with any additional risk factors should target maturity level three. At this level, organisations may consider using cyber security expertise to determine if some requirements are superseded by any security solutions or practices already in place.

To conclude the analogy, the car is now left with locked windows and doors, and an aftermarket alarm/immobilizer fitted. Opportunistic crime is prevented, and even dedicated criminals with experience and tools will be presented with a significant challenge when attempting to break in.

The Less Essential Twenty-Nine

When working with the Essential 8, it is important to remember that they are just the top eight mitigation strategies of a wider set of thirty-seven. While only eight made the ACSC's 'Essential' rating, many of the other twenty-nine strategies were still rated as 'Excellent', or 'Very Good'.

When working with organisations to improve their cyber security, we often find they are able to achieve better results for less investment by considering the other twenty-nine mitigation strategies than by pushing for a higher maturity level in the Essential 8.

An organisation which has only achieved a maturity level of one in the Essential 8 but implemented many of the other twenty-nine may be more secure than an organisation that has achieved a maturity level of three for the eight essential strategies, but not implemented any of the other twenty-nine.

Conclusion

There are several frameworks available to organisations looking to improve their cyber security, each with its own benefits and drawbacks; however, the Essential 8 is quickly becoming the de facto standard in Australia due to its heavy use in the public sector.

While larger organisations may find more value in focusing on other frameworks, a benchmark against the Essential 8 is still important.

For small and medium-sized enterprises, the Essential 8 provides a cost effective tool to understand and improve their cyber security practice without investing significant amounts of resource in security and compliance expertise.

Organisations using the Essential 8 should not disregard the ACSC's twenty-nine other mitigation strategies, which should also form a prominent part of their cyber security strategy.

The Essential 8 provides a fantastic entry point for organisations who want to begin to implement and mature modern cyber security defences, but who do not have strong internal compliance capabilities, or are unable to justify the cost of contracting these capabilities externally.

Full List of ACSC Mitigation Strategies

Essential (The Essential 8)	
Application control	Restrict administrative privileges
Patch applications	Patch operating systems.
Configure Microsoft Office macro settings	Multi-factor authentication
User application hardening.	Regular backups

Excellent	
Automated dynamic analysis of email and web content run in a sandbox	Disable local administrator accounts
Email content filtering	Network segmentation.
Web content filtering	Protect authentication credentials.
Deny corporate computers direct internet connectivity	Continuous incident detection and response
Operating system generic exploit mitigation	

Very Good	
Server application hardening	Outbound web and email data loss prevention.
Operating system hardening	Host-based intrusion detection/prevention system
Antivirus software using heuristics and reputation ratings	Endpoint detection and response software
Control removable storage media and connected devices.	Hunt to discover incidents
Block spoofed emails	Business continuity and disaster recovery plans
Non-persistent virtualised sandboxed environment	System recovery capabilities
Software-based application firewall, blocking incoming network traffic	Personnel management
Software-based application firewall, blocking outgoing network traffic	

Good
User education

Limited	
Antivirus software with up-to-date signatures	Network-based intrusion detection/ prevention system
TLS encryption between email servers	Capture network traffic

Contact Info

07 3326 2373

info@cyberguys.com.au

www.cyberguys.com.au

CYBERGUYS