CyberGuru

Business Without Interruption[™]

Cyber Security and IT: Protecting yourself and your family

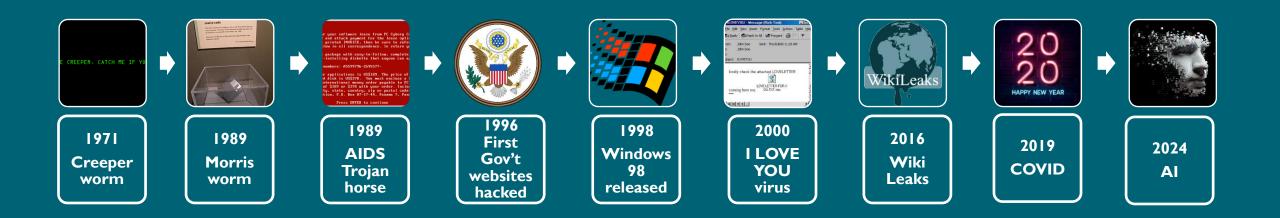
How CyberGuru began...





Significant dates

CyberGuru



Essential Eight Maturity Model

CyberGuru





Essential Eight Maturity Model

First published: June 2017 Last updated: November 2022



····

1

Introduction

The Australian Cyber Security Centre (ACSC) has developed prioritised mitigation strategies, in the form of the <u>Strategies to Mitigate Cyber Security incidents</u>, to help organisations protect themselves against various cyber threads. The most effective of these mitigation strategies are the Essential Eight.

The Essential Eight has been designed to protect Microsoft Windows-based internet-connected networks. While the principles behind the Essential Eight may be applied to cloud services and enterprise mobility, or other operating systems, it was not primarily designed for such purposes and alternative mitigation strategies may be more appropriate to mitigate unique cyber threats to these environments. In such cases, organisations should consider alternative guidance provided by the ACSC.

The <u>Essential Eight Maturity Model</u>, first published in June 2017 and updated regularly, supports the implementation of the Essential Eight. It is based on the ACSC's experience in producing other threat intelligence, responding to cyber security incidents, conducting penetration testing and assisting organisations to implement the Essential Eight.

Implementation

When implementing the Essential Eight, organisations should identify and plan for a target maturity level suitable for their environment. Organisations should then progressively implement each maturity level until that target is achieved

As the mitigation strategies that constitute the Essential Eight have been designed to complement each other, and to provide coverage of various cyber threats, organisations should plan their implementation to achieve the same maturity level across all eight mitigation strategies before moving onto higher maturity levels.

Organisations should implement the Essential Eight using a risk-based approach. In doing so, organisations should seek to minimise any exceptions and their scope, for example, by implementing compensating controls and ensuring the number of systems or users impacted are minimised. In addition, any exceptions, should be documented and approved through an appropriate process. Subsequently, the need for any exceptions, and associated compensating controls, should be monitored and reviewed on a regular basis. Note, the appropriate use of exceptions should not preclude an organisation from being assessed as meeting the requirements for a given maturity level.

As the Essential Eight outlines a minimum set of preventative measures, organisations need to implement additional measures to those within this maturity model where it is warranted by their environment. Further, while the Essential Eight can help to mitigate the majority of cyber threasts, it will not mitigate all cyber threasts. As such, additional mitigation strategies and controls need to be considered, including those from the <u>Strategies to Millioate Cyber</u> <u>Security incidentian and the information Security Monaul</u>.

- 1. Multi-factor authentication
- 2. Regular backups
- 3. Patch operating systems
- 4. Patch applications
- 5. Restrict administrative privileges
- 6. Application control
- 7. Configure Microsoft Office macro settings
- 8. User application hardening

Cyber Security today

 Think about your house/apartment where you live. You know exactly what you have to do to secure it and by doing those things you're confident it's secure.

• Now think about your digital house. What does it include?





Passwords



• Do not use the same password on more than one account.

• Purchase a password manager that enables you to store your account details securely. Do not use your website browser to store passwords.

• Enable multi-factor authentication on all possible accounts.

Security software



• Install commercial-grade security software on all devices, including desktops, laptops, tablets and phones (including iOS and Android).

• Ensure you regularly check for viruses and malware through scheduled scans.

 Configure a virtual private network (VPN) to access the internet when using WiFi hotspots.

Backups



• Perform regular backups of your files and store them in multiple locations.

• You may wish to store the data in locations other than your house (eg. bank safe custody box, trusted family member or friend, etc.).

• Use a cloud service such as OneDrive or Dropbox to store your files.

Updates



 Regularly update your computer's operating system, software and hardware.

• Where possible, configure automatic updates but check manually at least once a month.

• You may find these updates improve your devices' reliability and security.

Social engineering



 "The psychological manipulation of people into divulging information or performing actions for fraudulent purposes."

- Examples of social engineering include:
 - Phishing
 - Spear phishing
 - Vishing



Phishing email



SCAM



Australian Government

Australian Taxation Office

You have an outstanding refund from myGov.

Dear Costoner,

You have an exclusioning related here mySon, our transmitter management system detects that you are writted to wanter this payment.

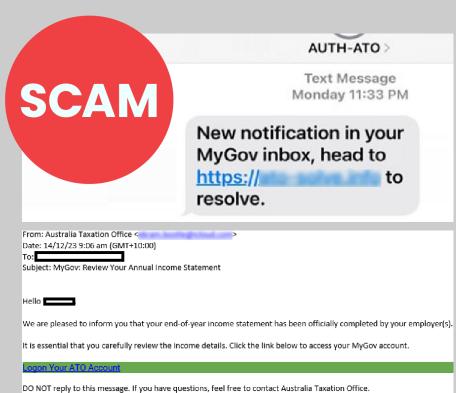
To accept fast payment orders rick on the following link and save the refund information:

Your rehard is available online : Assessmenthers

 Registration number 	 N/1208-7113483058)
- Amount	346.18 AUD
- Ortain	: Completed on the form

The confirmation must take place within the must 45 hours.

Phishing text



CyberGuru

Message reference: UE096

Sincerely,

The MyGov Team.

Vishing (Voice phishing)



"Microsoft Support" calling



Common organisations used by scammers

Via email:

- PayPal/Amazon
- eBay/Gumtree
- Australia Post
- ATO

- Via phone:
- Microsoft
- Telstra/Optus
- NBN
- Centrelink

Online shopping (tickets)

• Insurance



Start protecting yourself today



To reduce the likelihood of a cyber security incident, we recommend:

- 1. Setting up internet security software on all devices including mobile phones with a VPN if using WiFi hotspots.
- 2. Using strong passwords on your accounts, or better yet use a password manager.
- 3. Implementing multi-factor authentication on all websites and apps where possible. Install an authenticator such as Microsoft Authenticator or Google Authenticator.

Start protecting yourself today



To reduce the likelihood of cyber security issues, we recommend: (Continued)

- 4. Automating updates of your operating system, hardware and software.
- 5. Backing up your data on a regular basis in various locations (cloud, onsite and remotely).
- 6. Having a safe word that only you and family know. If you have a business, have another safe word to use among your team.

Useful links



Various websites are available to assist you in identifying and recovering from cyber security incidents, including:

- Australian Cyber Security Centre: https://www.cyber.gov.au/
- Stay Smart Online: <u>https://www.staysmartonline.gov.au/</u>
- ScamWatch: <u>https://www.scamwatch.gov.au/</u>
- IDCare: <u>https://www.idcare.org/</u>

Expression of interest

Are you interested in further sessions?

- Protecting and securing your devices
- Being efficient on the use of computers
- General computer housekeeping
- Artificial Intelligence (AI)



Contact us

Chris Jeffery

(07) 3185 0555

chris@cyberguru.com.au

www.cyberguru.com.au







Business Without Interruption[™]

Copyright 1997-2024 CyberGuru Pty Ltd All copyrights of images belong to their respective owners.