Australian Government
Australian Cyber Security Centre

ASD
AUSTRALIAN SIGNALS DIRECTORATE

PROTECT

FEBRUARY 2017

# Essential Eight Explained

The Australian Signals Directorate's (ASD) *Strategies to Mitigate Cyber Security Incidents* is a prioritised list of practical actions organisations can take to make their computers more secure. The advantage of this guidance is that it is customisable to each organisation based on their risk profile and the threats they are most concerned about.

## Introduction

1. The costs of compromise can be more expensive than preventative measures. Implementing the 'Essential Eight' mitigation strategies can save organisations considerable time, money, effort and reputational damage compared to cleaning up after a compromise.
2. While no single mitigation strategy is guaranteed to prevent cyber security incidents, ASD recommends organisations implement a package of eight essential strategies as a baseline. This baseline makes it much harder for adversaries to compromise systems.
3. Before implementing the strategies, organisations need to identify their assets and perform a risk assessment to identify the level of protection required from cyber threats.

   Organisations need to:

   a. Identify which assets require protection – do they hold important, sensitive or other information with a need for immediate and continuous access?

   b. Identify which adversaries are most likely to compromise their information – cyber criminals, nation-states or malicious insiders?

   c. Identify what level of protection is required – use the Essential Eight strategies as a baseline and then select other relevant strategies based on the risks to their business.
4. There is a suggested order of implementation for each threat to build a defence-in-depth cyber security posture. Once the Essential Eight mitigation strategies on page 2 of this document have been correctly implemented, a baseline cyber security posture has been achieved.
5. More detail, strategies and implementation guidance is available from: www.asd.gov.au/infosec/mitigationstrategies
6. If you are the victim of a cyber security incident, please report it to:
   - Australian government organisations: ASD www.asd.gov.au/infosec/reportincident
   - Australian businesses: email CERT Australia info@cert.gov.au
   - Australian individuals: Australian Cybercrime Online Reporting Network: www.acorn.gov.au

# The Essential Eight

## To prevent malware running:

| | |
|---|---|
| **Application Whitelisting** [TOP 4]<br>A whitelist only allows selected software applications to run on computers.<br>***Why?*** All other software applications are stopped, including malware. | **Patch Applications** [TOP 4]<br>A patch fixes security vulnerabilities in software applications.<br>***Why?*** Adversaries will use known security vulnerabilities to target computers. |
| **Disable untrusted Microsoft Office macros**<br>Microsoft Office applications can use software known as “macros” to automate routine tasks.<br>***Why?*** Macros are increasingly being used to enable the download of malware. Adversaries can then access sensitive information, so macros should be secured or disabled. | **User application hardening**<br>Block web browser access to Adobe Flash player (uninstall if possible), web advertisements and untrusted Java code on the internet.<br>***Why?*** Flash, Java and web ads have long been popular ways to deliver malware to infect computers. |

## To limit the extent of incidents and recover data:

| | |
|---|---|
| **Restrict administrative privileges** [TOP 4]<br>Only use administrator privileges for managing systems, installing legitimate software and applying software patches. These should be restricted to only those that need them.<br>***Why?*** Admin accounts are the ‘keys to the kingdom’, adversaries use these accounts for full access to information and systems. | **Patching operating systems** [TOP 4]<br>A patch fixes security vulnerabilities in operating systems.<br>***Why?*** Adversaries will use known security vulnerabilities to target computers. |
| **Multi-factor authentication**<br>This is when a user is only granted access after successfully presenting multiple, separate pieces of evidence. Typically:<br>Something you know, like a passphrase.<br>Something you have, like a physical token.<br>And/or something you are, like biometric data.<br>***Why?*** Having multiple levels of authentication makes it a lot harder for adversaries to access your information. | **Daily backup of important data**<br>Regularly back up all data and store it securely offline.<br>***Why?*** That way your organisation can access data again if it suffers a cyber security incident. |

[TOP 4] strategies to mitigate targeted cyber intrusions