INFS 5115 Security Principles

# Defence-in-depth

University of South Australia

School of
Information Technology
and Mathematical Sciences

# Defence-in-depth

- In this module, we will review the topic of cybersecurity defence-in-depth, including contemporary definitions and analogies with physical security measures.
- We will also discuss a selection of the Australian Signal Directorate's 'Strategies to Mitigate Cyber Security Incidents' to gain an understanding of the types of mitigations that may be used as part of a defence-in-depth strategy, and the rationale for implementing each potential mitigation.

# Defence-in-depth

Definition

- Defence-in-Depth
  - *Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization.*[1]
- *In contrast to:* Defence-in-Breadth
  - *A planned, systematic set of multidisciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or sub-component life cycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement).*[1]

[1] CNSSI-4009 cited in Kissel, R., 2013. Glossary of Key Information Security Terms. NIST Interagency Reports, NISTIR 7298.

# Defence-in-depth

- Defence-in-depth
  - describes the implementation of multiple diverse safeguards at different layers of the entity being protected
  - requires adversaries to successfully defeat multiple mechanisms and decreases the likelihood of a successful attack
  - increases the likelihood of detection
- The number of security layers implemented should be dependent on the importance of the asset being protected from the business' perspective.

NIST 2015, 'Security and Privacy Controls for Federal Information Systems and Organizations', National Institute of Standards and Technology, SP 800-53r4.

# Defence-in-depth

Practical Analogy

- Why is a bank typically more secure than a convenience store?

# Defence-in-depth

Practical Analogy

- ***Security cameras*** *alone are a deterrent for some. But if people don't care about the cameras, then a* ***security guard*** *is there to physically defend the bank with a gun.* ***Two security guards*** *provide even more protection. But if both security guards get shot by masked bandits, then at least there's still a* ***wall of bulletproof glass*** *and* ***electronically locked doors*** *to protect the tellers from the robbers.*
- *Of course if the robbers happen to kick in the doors, or guess the code for the door, at least they can only get at the teller registers, since we have a* ***vault*** *protecting the really valuable stuff. Hopefully, the vault is protected by* ***several locks****, and cannot be opened without* ***two individuals*** *who are rarely at the bank at the same time. And as for the teller registers, they can be protected by having* ***dye-emitting bills*** *stored at the bottom, for distribution during a robbery.*
- *Having all these security measures does not ensure that our bank will never be successfully robbed. Bank robberies do happen, even at banks with this much security.*

Viega and McGraw cited in US-CERT 2005, ‘Defence in Depth’, https://www.us-cert.gov/bsi/articles/knowledge/principles/defense-in-depth

# Defence-in-depth

- The first stage of implementing a defence-in-depth strategy is knowing the assets that exist in the corporate network.
  - Automated tools can be used to monitor the assets connected to the network.
- All individual devices must then be secured.
  - This includes all routers, switches and other network/systems equipment.
- Once the devices themselves have been secured, all points of access to the hosts must be examined.
  - Data that traverses between certain internal networks, and any internal network and the internet should pass through network security devices for inspection.

Harley, D 2007, AVIEN malware defense guide for the Enterprise, Syngress, Burlington, MA.

# Defence-in-depth

Activity 1

Secure The Network Using Defence-In-Depth Stage 1 – Infrastructure

Consider these two points from the previous slide when working on the activity.

- All individual devices must then be secured.
- Data that traverses between **certain** internal networks, and any internal network and the internet should pass through network security devices for inspection

Harley, D 2007, AVIEN malware defense guide for the Enterprise, Syngress, Burlington, MA.

# Defence-in-depth

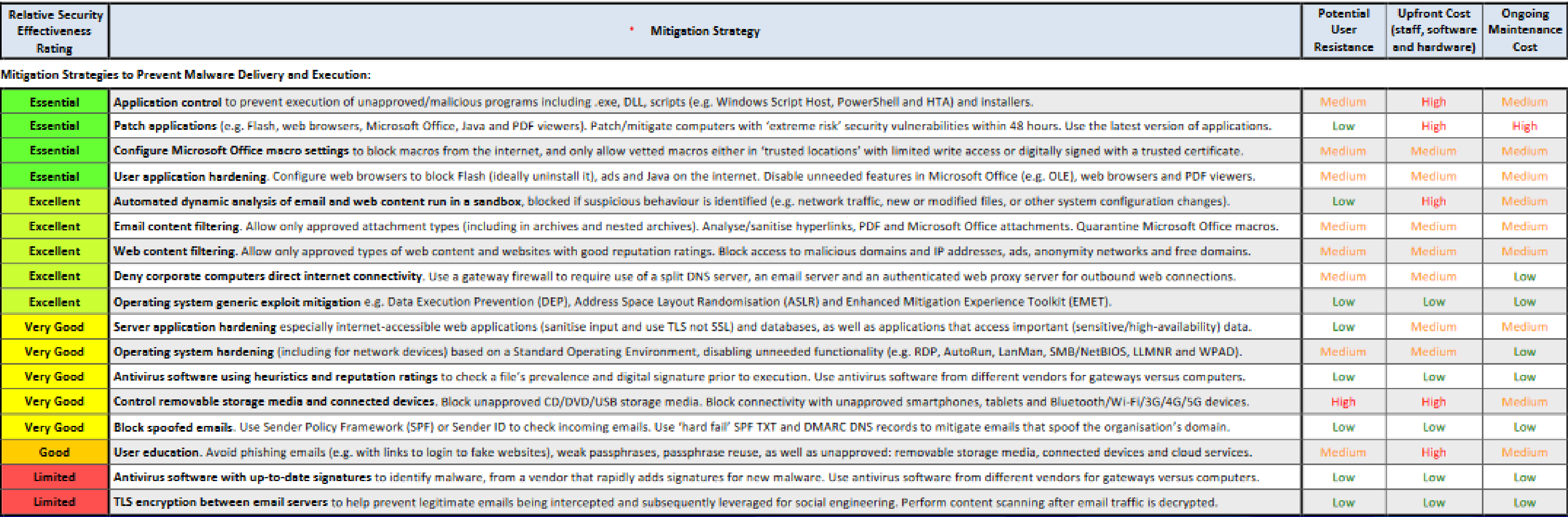
- The principle of least privilege and principle of least functionality are integral to defence-in-depth.

Harley, D 2007, AVIEN malware defense guide for the Enterprise, Syngress, Burlington, MA.

# ASD Mitigation Strategies

- One source of mitigation strategies that can provide a basis for the implementation of a defence-in-depth strategy is the ASD’s Strategies to Mitigate Cyber Security Incidents (mitigation strategies).
- **You should read the ASD Strategies to Mitigate Cyber Security Incidents documents (links available on the course website) and familiarise yourself with each strategy (in particular, the Essential 8), its associated rationale and a basic understanding of the implementation process**

# ASD Mitigation Strategies (example)



| Relative Security Effectiveness Rating | * Mitigation Strategy | Potential User Resistance | Upfront Cost (staff, software and hardware) | Ongoing Maintenance Cost |
|---|---|---|---|---|
| Mitigation Strategies to Prevent Malware Delivery and Execution: | | | | |
| Essential | **Application control** to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers. | Medium | High | Medium |
| Essential | **Patch applications** (e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers). Patch/mitigate computers with 'extreme risk' security vulnerabilities within 48 hours. Use the latest version of applications. | Low | High | High |
| Essential | **Configure Microsoft Office macro settings** to block macros from the internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate. | Medium | Medium | Medium |
| Essential | **User application hardening**. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers. | Medium | Medium | Medium |
| Excellent | **Automated dynamic analysis of email and web content run in a sandbox**, blocked if suspicious behaviour is identified (e.g. network traffic, new or modified files, or other system configuration changes). | Low | High | Medium |
| Excellent | **Email content filtering**. Allow only approved attachment types (including in archives and nested archives). Analyse/sanitise hyperlinks, PDF and Microsoft Office attachments. Quarantine Microsoft Office macros. | Medium | Medium | Medium |
| Excellent | **Web content filtering**. Allow only approved types of web content and websites with good reputation ratings. Block access to malicious domains and IP addresses, ads, anonymity networks and free domains. | Medium | Medium | Medium |
| Excellent | **Deny corporate computers direct internet connectivity**. Use a gateway firewall to require use of a split DNS server, an email server and an authenticated web proxy server for outbound web connections. | Medium | Medium | Low |
| Excellent | **Operating system generic exploit mitigation** e.g. Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR) and Enhanced Mitigation Experience Toolkit (EMET). | Low | Low | Low |
| Very Good | **Server application hardening** especially internet-accessible web applications (sanitise input and use TLS not SSL) and databases, as well as applications that access important (sensitive/high-availability) data. | Low | Medium | Medium |
| Very Good | **Operating system hardening** (including for network devices) based on a Standard Operating Environment, disabling unneeded functionality (e.g. RDP, AutoRun, LanMan, SMB/NetBIOS, LLMNR and WPAD). | Medium | Medium | Low |
| Very Good | **Antivirus software using heuristics and reputation ratings** to check a file's prevalence and digital signature prior to execution. Use antivirus software from different vendors for gateways versus computers. | Low | Low | Low |
| Very Good | **Control removable storage media and connected devices**. Block unapproved CD/DVD/USB storage media. Block connectivity with unapproved smartphones, tablets and Bluetooth/Wi-Fi/3G/4G/5G devices. | High | High | Medium |
| Very Good | **Block spoofed emails**. Use Sender Policy Framework (SPF) or Sender ID to check incoming emails. Use 'hard fail' SPF TXT and DMARC DNS records to mitigate emails that spoof the organisation's domain. | Low | Low | Low |
| Good | **User education**. Avoid phishing emails (e.g. with links to login to fake websites), weak passphrases, passphrase reuse, as well as unapproved: removable storage media, connected devices and cloud services. | Medium | High | Medium |
| Limited | **Antivirus software with up-to-date signatures** to identify malware, from a vendor that rapidly adds signatures for new malware. Use antivirus software from different vendors for gateways versus computers. | Low | Low | Low |
| Limited | **TLS encryption between email servers** to help prevent legitimate emails being intercepted and subsequently leveraged for social engineering. Perform content scanning after email traffic is decrypted. | Low | Low | Low |

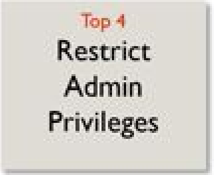
University of
South Australia

School of
Information Technology
and Mathematical Sciences

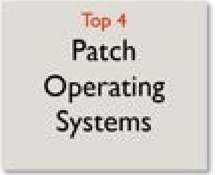
Australian Signals Directorate 2017, 'Strategies to Mitigate Cyber Security Incidents', https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents, n.p.

# ASD Mitigation Strategies

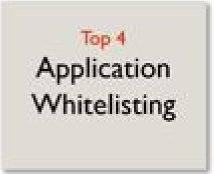
- Properly implementing the ‘Top 4’ strategies will mitigate over 85% of targeted threats, as assessed by the ASD.



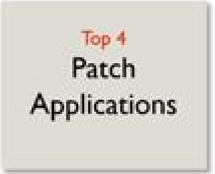
Top 4
Restrict Admin Privileges



Top 4
Patch Operating Systems



Top 4
Application Whitelisting



Top 4
Patch Applications

- The ‘Essential 8’ mitigation strategies are considered baseline security.
- In this presentation we will briefly outline the ‘Essential 8’ mitigation strategies.

Australian Signals Directorate 2017, ‘Strategies to Mitigate Cyber Security Incidents’, https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents

# ACSC Mitigation Strategies

## Maturity Levels

To assist organisations in determining the maturity of their implementation of the Essential Eight, three maturity levels have been defined for each mitigation strategy. The maturity levels are defined as:

- Maturity Level One: Partly aligned with the intent of the mitigation strategy
- Maturity Level Two: Mostly aligned with the intent of the mitigation strategy
- Maturity Level Three: Fully aligned with the intent of the mitigation strategy.

Australian Signals Directorate, *Essential Eight Maturity Model*, https://www.cyber.gov.au/acsc/view-all-content/essential-eight/essential-eight-maturity-model

# ASD Mitigation Strategies

Application Control

- *Application control to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTML Applications) and installers.*[1]
- Application whitelisting is a type of host based protection that prevents adversaries from executing non-approved software.
- For example, it can potentially prevent initial malware infection by stopping the infected executable code from running.
- On more privileged hosts, it may prevent attackers from utilising tools that may help steal credentials or escalate privileges.

Australian Signals Directorate 2017, 'Strategies to Mitigate Cyber Security Incidents – Mitigation Details', https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents-mitigation-details

[1] ibid, n.p.

# ASD Mitigation Strategies

## Whitelisting vs Blacklisting

- Many traditional security tools relied upon blacklisting of malicious network traffic or software.
  - This approach is reactive and provides limited security.
  - Adversaries are often able to change their behaviour to evade blacklists quite quickly, turning security into a ‘cat-and-mouse game’.
  - Whitelisting is generally a more appropriate approach, whereby all activity is denied, unless it is specifically approved.
  - Generally approval is only granted for a specific business purpose.

Australian Signals Directorate 2017, ‘Strategies to Mitigate Cyber Security Incidents – Mitigation Details’, https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents-mitigation-details

# ACSC Mitigation Strategies

## Maturity Levels

### Application Control

| Maturity Level One | Maturity Level Two | Maturity Level Three |
|---|---|---|
| An application whitelisting solution is implemented on all workstations to restrict the execution of executables to an approved set.<br>An application whitelisting solution is implemented on all servers to restrict the execution of executables to an approved set. | An application whitelisting solution is implemented on all workstations to restrict the execution of executables, software libraries, scripts and installers to an approved set.<br>An application whitelisting solution is implemented on all servers to restrict the execution of executables, software libraries, scripts and installers to an approved set. | Includes all mitigations from Level 1 and 2 plus:<br>Microsoft's latest recommended block rules are implemented to prevent application whitelisting bypasses.<br>https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules |

Australian Signals Directorate, *Essential Eight Maturity Model*, https://www.cyber.gov.au/acsc/view-all-content/essential-eight/essential-eight-maturity-model

# ASD Mitigation Strategies

## Patch applications

- Patch applications, particularly those used for internet communications or for opening email attachments.
- Both client and server applications need to be considered and patched.
- Computers exposed to ‘extreme risk’ vulnerabilities should be patched within 48 hours of the vulnerability being identified.
- These types of vulnerabilities may allow an adversary to execute malicious code.
- A strategy for upgrading application versions should be implemented, as older software generally reaches a stage where it is no longer supported with patches for security vulnerabilities.

Australian Signals Directorate 2017, ‘Strategies to Mitigate Cyber Security Incidents – Mitigation Details’, https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents-mitigation-details

# ASD Mitigation Strategies

## Patch applications

**An Example:**

Google is hurrying out a fix for a vulnerability in its Chrome browser that's under active attack – its third zero-day flaw so far this year. If exploited, the flaw could allow remote code-execution and denial-of-service attacks on affected systems.
The vulnerability exists in Blink, the browser engine for Chrome developed as part of the Chromium project. Browser engines convert HTML documents and other web page resources into the visual representations viewable to end users.

**Search for Common Vulnerabilities and Exposures here**: https://nvd.nist.gov/vuln/search

Search for this CVE-2021-21193

Australian Signals Directorate 2017, 'Strategies to Mitigate Cyber Security Incidents – Mitigation Details', https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents-mitigation-details

# ACSC Mitigation Strategies

## Patch applications

| Maturity Level One | Maturity Level Two | Maturity Level Three |
|---|---|---|
| Security vulnerabilities in applications and drivers assessed as extreme risk are patched, updated or mitigated within one month of the security vulnerabilities being identified by vendors, independent third parties, system managers or users.<br>Applications that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions. | Same as Level one but patched within two weeks | Same as Level two but patched within 48 hours<br>AND<br>An automated mechanism is used to confirm and record that deployed application and driver patches or updates have been installed, applied successfully and remain in place. |

Australian Signals Directorate, *Essential Eight Maturity Model*, https://www.cyber.gov.au/acsc/view-all-content/essential-eight/essential-eight-maturity-model

# ASD Mitigation Strategies

## Patch Operating Systems

- The guidance for patching operating systems is similar to that for patching applications.
- Operating system vulnerabilities can be exploited to allow actions such as escalation of privileges.
- ASD provides guidance on applying patches based on a risk management approach that takes into account the severity and potential business impact of associated vulnerabilities.

Examples:

CVE-2021-27070 - Windows 10 Update Assistant Elevation of Privilege Vulnerability

CVE-2021-24106 - Windows DirectX Information Disclosure Vulnerability

Australian Signals Directorate 2017, 'Strategies to Mitigate Cyber Security Incidents – Mitigation Details', https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents-mitigation-details

# ACSC Mitigation Strategies

## Patch Operating Systems

| Maturity Level One | Maturity Level Two | Maturity Level Three |
|---|---|---|
| Security vulnerabilities in operating systems and firmware assessed as extreme risk are patched, updated or mitigated within one month of the security vulnerabilities being identified by vendors, independent third parties, system managers or users.<br>Operating systems for workstations, servers and ICT equipment that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions. | Same as Level one but patched within two weeks | Same as Level two but patched within 48 hours<br>AND<br>An automated mechanism is used to confirm and record that deployed operating system and firmware patches or updates have been installed, applied successfully and remain in place. |

Australian Signals Directorate, *Essential Eight Maturity Model*, https://www.cyber.gov.au/acsc/view-all-content/essential-eight/essential-eight-maturity-model

# ASD Mitigation Strategies

- *Configure Microsoft Office macro settings to block macros from the Internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.*[1]
- Microsoft Office macros can be leveraged to execute malicious code on devices and may bypass basic email filtering and application whitelisting implementations.

Example Spearphishing Attachment:

https://attack.mitre.org/techniques/T1566/001/

Australian Signals Directorate 2017, ‘Strategies to Mitigate Cyber Security Incidents – Mitigation Details’, https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents-mitigation-details

[1] ibid, n.p.

# ACSC Mitigation Strategies

## Configure Microsoft Office macro settings

| Maturity Level One | Maturity Level Two | Maturity Level Three |
|---|---|---|
| Microsoft Office macros are allowed to execute, but only after prompting users for approval.<br>Microsoft Office macro security settings cannot be changed by users. | Only signed Microsoft Office macros are allowed to execute.<br>Microsoft Office macros in documents originating from the internet are blocked.<br>Microsoft Office macro security settings cannot be changed by users. | Microsoft Office macros are only allowed to execute in documents from Trusted Locations where write access is limited to personnel whose role is to vet and approve macros.<br>Microsoft Office macros in documents originating from the internet are blocked.<br>Microsoft Office macro security settings cannot be changed by users. |

University of South Australia

School of Information Technology and Mathematical Sciences

Australian Signals Directorate, *Essential Eight Maturity Model*, https://www.cyber.gov.au/acsc/view-all-content/essential-eight/essential-eight-maturity-model

# ASD Mitigation Strategies

- Examples include: *Configure web browsers to block Flash (ideally uninstall it if possible), advertisements and untrusted Java code on the Internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.*[1]
- This helps to reduce the potential attack vectors that an adversary can exploit and their ability to evade other security measures, such as application whitelisting.

Australian Signals Directorate 2017, 'Strategies to Mitigate Cyber Security Incidents – Mitigation Details', https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents-mitigation-details

[1] ibid, n.p.

# ACSC Mitigation Strategies

User application hardening

| Maturity Level One | Maturity Level Two | Maturity Level Three |
|---|---|---|
| Web browsers are configured to block or disable support for Flash content. | Same as Level 1 plus<br>Web browsers are configured to block web advertisements.<br>Web browsers are configured to block Java from the internet. | Same as Level 2 plus<br>Microsoft Office is configured to disable support for Flash content.<br>Microsoft Office is configured to prevent activation of Object Linking and Embedding packages. |

Australian Signals Directorate, *Essential Eight Maturity Model*, https://www.cyber.gov.au/acsc/view-all-content/essential-eight/essential-eight-maturity-model

# ASD Mitigation Strategies

**Restrict administrative privileges**

- *Restrict administrative privileges to operating systems and applications based on user duties. Validate the requirement for users to be granted administrative privileges, and revalidate this requirement at least annually and preferably monthly.*[1]
- If a non-privileged account is compromised, the consequences should be reduced in comparison to the compromise of a privileged account.
- Privileged users should use a separate unprivileged account, and preferably physical workstation, for non-administrative or risky activities (e.g. email, web browsing).

Example:

https://www.windowscentral.com/how-use-windows-10-non-admin-and-why#:~:text=Double%2Dclick%20your%20Windows%2010,Click%20the%20Remove%20button.

Australian Signals Directorate 2017, 'Strategies to Mitigate Cyber Security Incidents – Mitigation Details', https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents-mitigation-details

[1] ibid, n.p.

# ACSC Mitigation Strategies

Restrict administrative privileges

| Maturity Level One | Maturity Level Two | Maturity Level Three |
|---|---|---|
| Privileged access to systems, applications and data repositories is validated when first requested.<br>Policy security controls are used to prevent privileged users from reading emails, browsing the web and obtaining files via online services | Same as Level 1 plus<br>Privileged access to systems, applications and data repositories is validated when first requested and revalidated on an annual or more frequent basis. | Same as Level 2 plus<br>Privileged access to systems, applications and data repositories is limited to that required for personnel to undertake their duties.<br>Technical security controls are used to prevent privileged users from reading emails, browsing the web and obtaining files via online services. |

Australian Signals Directorate, *Essential Eight Maturity Model*, https://www.cyber.gov.au/acsc/view-all-content/essential-eight/essential-eight-maturity-model

# ASD Mitigation Strategies

Multi-factor authentication

- The concept of multi-factor authentication was discussed in Module 1.
- It should be implemented on most likely targets, remotely accessed systems, and when privileged access is required or requests are made for data stored in a sensitive data repository.
- Multi-factor authentication can make it substantially more difficult for adversaries to utilise stolen user credentials.

Australian Signals Directorate 2017, ‘Strategies to Mitigate Cyber Security Incidents – Mitigation Details’, https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents-mitigation-details

# ACSC Mitigation Strategies

## Multi-factor authentication

| Maturity Level One | Maturity Level Two | Maturity Level Three |
|---|---|---|
| Multi-factor authentication uses at least two of the following authentication factors:<br>Passwords, Universal 2nd Factor security keys, physical one-time password tokens, biometrics, smartcards, mobile app one-time password tokens, SMS messages, emails, voice calls or software certificates. | Same as Level 1 plus<br>Multi-factor authentication is used to authenticate all users of remote access solutions.<br>Multi-factor authentication is used to authenticate all privileged users and any other positions of trust. | Same as Level 2 plus<br>Multi-factor authentication is used to authenticate all users when accessing important data repositories. |

Australian Signals Directorate, *Essential Eight Maturity Model*, https://www.cyber.gov.au/acsc/view-all-content/essential-eight/essential-eight-maturity-model

# ASD Mitigation Strategies

## Daily Backups

- *Daily backups of important new/changed data, software and configuration settings, stored disconnected and retained for at least three months.*[1]
- *Test the restoration process when the backup capability is initially implemented, annually and whenever IT infrastructure changes.*[1]
- Backups are integral for data restoration purposes after a cybersecurity event.
- This can include malicious events, such as a ransomware infection, and non-malicious events, such as user error.

Australian Signals Directorate 2017, ‘Strategies to Mitigate Cyber Security Incidents – Mitigation Details’, https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents-mitigation-details

[1] ibid, n.p.

# ACSC Mitigation Strategies

## Daily Backups

| Maturity Level One | Maturity Level Two | Maturity Level Three |
|---|---|---|
| Backups of important information, software and configuration settings are performed monthly.<br>Backups are stored for between one to three months.<br>Partial restoration of backups is tested on an annual or more frequent basis. | Same as Level 1 plus<br>Backups of important information, software and configuration settings are performed weekly.<br>Backups are stored offline, or online but in a non-rewritable and non-erasable manner.<br>Full restoration of backups is tested at least once and partial restoration of backups is tested on a bi-annual | Same as Level 2 plus<br>Backups of important information, software and configuration settings are performed at least daily.<br>Backups are stored for three months or greater.<br>Full restoration of backups is tested at least once when initially implemented and each time fundamental information technology infrastructure changes occur.<br>Partial restoration of backups is tested on a quarterly or more frequent basis. |

Australian Signals Directorate, *Essential Eight Maturity Model*, https://www.cyber.gov.au/acsc/view-all-content/essential-eight/essential-eight-maturity-model

# ACSC Mitigation Strategies

1. Mitigation Strategies to Prevent Malware Delivery and Execution
2. Mitigation Strategies to Limit the Extent of Cyber Security Incidents
3. Mitigation Strategies to Detect Cyber Security Incidents and Respond
4. Mitigation Strategies to Recover Data and System Availability
5. Mitigation Strategy Specific to Malicious Insiders

Australian Signals Directorate, *Essential Eight Maturity Model*, https://www.cyber.gov.au/acsc/view-all-content/essential-eight/essential-eight-maturity-model