1. The Australian Signals Directorate (ASD) has developed prioritised mitigation strategies to help technical cyber security professionals in all organisations mitigate cyber security incidents caused by various threats. This guidance addresses targeted cyber intrusions (e.g. executed by advanced persistent threats such as foreign intelligence services), ransomware and external adversaries with destructive intent, malicious insiders, “business email compromise”, and industrial control systems.

2. This guidance is informed by ASD’s experience responding to cyber security incidents, performing vulnerability assessments and penetration testing Australian government organisations.

3. Prior to implementing mitigation strategies, organisations need to identify their assets and perform a risk assessment to identify the level of protection required from various threats. Organisations require motivation to improve their cyber security posture, supportive executives, access to skilled cyber security professionals and adequate financial resources. Motivators include a detected cyber security incident, a penetration test, mandatory data breach reporting, mandatory compliance, and evidence of a lower cyber security posture or higher threat exposure than previously realised.

4. The following page provides the mitigation strategies and a suggested implementation order for:
   - targeted cyber intrusions and other external adversaries who steal data
   - ransomware denying access to data for monetary gain, and external adversaries who destroy data and prevent computers/networks from functioning
   - malicious insiders who steal data such as customer details or intellectual property
   - malicious insiders who destroy data and prevent computers/networks from functioning.

5. When implementing a mitigation strategy, first implement it for high risk users and computers such as those with access to important (sensitive or high-availability) data and exposed to untrustworthy Internet content, and then implement it for all other users and computers. Organisations should perform hands-on testing to verify the effectiveness of their implementation of mitigation strategies.

6. No single mitigation strategy is guaranteed to prevent cyber security incidents. Properly implementing application whitelisting, patching applications, patching operating systems and restricting administrative privileges (referred to as the Top 4) continues to mitigate over 85% of adversary techniques used in targeted cyber intrusions which ASD has visibility of.

7. Incorporating the Top 4, the eight mitigation strategies with an “essential” effectiveness rating are so effective at mitigating targeted cyber intrusions and ransomware, that ASD considers them to be the cyber security baseline for all organisations. Any organisation that has been compromised despite properly implementing these mitigation strategies is encouraged to notify ASD.

8. The companion Strategies to Mitigate Cyber Security Incidents – Mitigation Details document contains updated implementation guidance for the mitigation strategies, as well as new guidance to mitigate “business email compromise” and threats to industrial control systems.

9. ASD’s Australian Government Information Security Manual (ISM) provides supporting guidance. The ISM and additional guidance are available on ASD’s website at http://www.asd.gov.au. ASD’s website also has separate and specific guidance for mitigating denial of service, and securely using cloud computing and enterprise mobility including personally owned computing devices.
### Mitigation Strategies to Prevent Malware Delivery and Execution:

| Essential | Application whitelisting of approved/approved programs to prevent execution of unapproved/untrusted applications, including app.exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers. | Medium | High | Medium |
| Essential | Patch operating systems, patch/mitigate computers (including network devices) with "extreme risk" vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions. | Medium | Medium | Low |
| Essential | Configure Microsoft Office macro settings to block macros in Excel and Access files, and only allow visited macros either in "trusted locations" with limited write access or digitally signed with a trusted certificate. | Low | Medium | Medium |
| Essential | User education and awareness. Inform users to be wary of or avoid clicking suspicious links, phishing attempts, or opening untrusted email attachments. | Low | Low | Low |
| Essential | Automated dynamic analysis of email and web content: block/whitelist suspicious behaviour and email addresses (e.g. network traffic, new or modified files, or other system configuration changes). | Medium | Medium | Medium |
| Essential | Email content filtering. Whitelist allowed attachment types (e.g. in archives and network drives). Use antispam software to analyse web content and websites with good reputation. | Medium | Medium | Medium |

### Malicious Insiders who steal data:

1. Implement 'Control' removable media and connected devices to mitigate data exfiltration.
2. Implement 'Output' web and email data loss prevention strategies.
3. Implement 'Essential' mitigation strategies to: a) recover data and system availability b) prevent malware delivery and execution c) detect cyber security incidents and respond.
4. Repeat step 3 with less effective mitigation strategies until an acceptable level of residual risk is reached.

Note: 'Hunt to discover incidents' is less relevant for malicious insiders that immediately make itself visible.

### Mitigation Strategies to Detect Malicious Insiders:

1. Implement 'Control' removable media and connected devices to mitigate data exfiltration.
2. Implement 'Output' web and email data loss prevention strategies.
3. Implement 'Essential' mitigation strategies to: a) recover data and system availability b) prevent malware delivery and execution c) detect cyber security incidents and respond.
4. Repeat step 3 with less effective mitigation strategies until an acceptable level of residual risk is reached.

### Ransomware and external adversaries who destroy data and prevent computers/networks from functioning:

1. Implement 'Essential' mitigation strategies to: a) recover data and system availability b) prevent malware delivery and execution c) detect cyber security incidents and respond.
2. Repeat step 1 with less effective mitigation strategies until an acceptable level of residual risk is reached.

Note: 'Hunt to discover incidents' is less relevant for ransomware that immediately makes itself visible.

### Mitigation Strategies to Detect and Prevent Malicious Insiders:

- **Essential**: Identify and investigate suspicious activities and patterns. Use automated monitoring tools to detect anomalies, such as unusual file access, network connections, or process creation.
- **Medium**: Implement intrusion detection/prevention tools, such as Network-Based Intrusion Detection Systems (NIDS) or Host-Based Intrusion Prevention Systems (HIDS), to monitor network traffic and detect suspicious activities.
- **Low**: Conduct regular system scans and audits to identify vulnerabilities and ensure that security controls are configured correctly.

### Mitigation Strategies to Prevent Malware Delivery and Execution:

- **Essential**: Prevent malware delivery and execution by implementing a comprehensive patch management strategy and keeping all systems up to date.
- **Medium**: Implement user education and awareness programs to inform users about the risks of downloading and installing untrusted software.
- **Low**: Use antivirus software to scan files and prevent malware from executing.

### Mitigation Strategies to Detect Malicious Insiders:

- **Essential**: Use Intrusion Detection Systems (IDS) to monitor network traffic for suspicious activity.
- **Medium**: Implement user education and awareness programs to inform users about the risks of downloading and installing untrusted software.
- **Low**: Use antivirus software to scan files and prevent malware from executing.

---

**Suggested Mitigation Strategy Implementation Order**

<table>
<thead>
<tr>
<th>Targeted Cyber Intrusions and Other External Adversaries who Steal Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Implement &quot;Essential&quot; mitigation strategies to: a. Prevent malware delivery and execution b. Limit the extent of cyber security incidents c. Detect cyber security incidents and respond. 2. Repeat step 1 with &quot;Essential&quot; mitigation strategies. 3. Repeat step 1 with less effective mitigation strategies until an acceptable level of residual risk is reached.</td>
</tr>
</tbody>
</table>
Summary of key changes for 2017

10. The title and scope of the document have been updated to mitigate additional threats. Three new mitigation strategies to recover data and system availability help mitigate ransomware. The new mitigation strategies ‘Personnel management’ and ‘Outbound web and email data loss prevention’ help mitigate malicious insiders. The Strategies to Mitigate Cyber Security Incidents – Mitigation Details document, hereafter referred to as “the Mitigation Details document”, has new guidance for these threats as well as for “business email compromise” and industrial control systems.

11. The leftmost numerical ranking column was being misinterpreted by some readers, and has been converted into a suggested mitigation strategy implementation order for each threat, providing a principles-based approach to building a defence-in-depth cyber security posture.

12. The rightmost four columns (e.g. “Helps Prevent Intrusion Stage 1: Code Execution”) have been converted into category headings (e.g. “Mitigation Strategies to Prevent Malware Delivery and Execution”). Mitigation strategies have been categorised based on their primary security outcome.

13. Effectiveness ratings now include “very good”, while “average” has been changed to “limited”.

14. Mitigation strategy ‘Application whitelisting’ now mentions Windows Script Host, PowerShell and HTML Applications (HTA). Further guidance has been added to the Mitigation Details document.

15. The two patching mitigation strategies now reference ASD’s definition of “extreme risk” vulnerabilities to reflect that the 48 hour (previously two day) timeframe to apply patches doesn’t apply to every vulnerability affecting every computer. The list of applications has been reordered since Flash, web browsers and Microsoft Office are exploited more than Java and PDF viewers.

16. New mitigation strategy ‘Configure Microsoft Office macro settings’ has been extracted from mitigation strategy ‘User application hardening’ to reflect the prevalence of malicious Microsoft Office macros. ASD has witnessed our guidance mitigate attempts to compromise Australian organisations by adversaries working for a foreign intelligence service.

17. Mitigation strategy ‘User application hardening’ is now rated “essential” and advises to uninstall Adobe Flash if possible, disable Microsoft Office OLE packages, and block Internet ads due to malicious advertising (malvertising). Some organisations might choose to support selected websites that rely on ads for revenue by enabling just their ads and potentially risking compromise.

18. Mitigation strategy ‘Multi-factor authentication’ is now rated “essential” to reflect the prevalence of passphrase theft and the abuse of remote access for infiltration, data exfiltration and persistence.

19. Mitigation strategy ‘Enforce a strong passphrase policy’ has been renamed to ‘Protect authentication credentials’, contains specific new guidance and is now rated “excellent”.

20. The two logging mitigation strategies have been combined into mitigation strategy ‘Continuous incident detection and response’. Also, while the key goal remains to identify and protect assets to prevent cyber security incidents, two new mitigation strategies reduce the time to detect and respond to such incidents – ‘Endpoint detection and response software’ and ‘Hunt to discover incidents’ leveraging threat intelligence, with details added to the Mitigation Details document.

21. Mitigation strategy ‘Server application hardening’ is now rated “very good” to reflect an increase in cyber security incidents involving web servers compromised with web shells.

22. Mitigation strategy ‘Block spoofed emails’ now advises to configure DMARC DNS records.

23. Mitigation strategies ‘Web domain whitelisting for all domains’, ‘Block attempts to access websites by their IP address’ and ‘Gateway blacklisting’ have merged into ‘Web content filtering’.

24. Mitigation strategies ‘Restrict access to Server Message Block (SMB) and NetBIOS’ and ‘Workstation inspection of Microsoft Office files’ have merged with existing mitigation strategies.

Contact details

25. Australian government customers with questions regarding this advice should contact ASD Advice and Assistance by emailing asd.assist@defence.gov.au or by calling 1300 CYBER1 (1300 292 371).

26. Australian businesses or other private sector organisations with questions regarding this advice should contact CERT Australia by emailing info@cert.gov.au or by calling 1300 172 499.