Introduction

The Australian Cyber Security Centre (ACSC) has developed prioritised mitigation strategies to help cyber security professionals in all organisations mitigate cyber security incidents caused by various cyber threats. This guidance addresses targeted cyber intrusions (i.e. those 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.

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

Prior to implementing any of the mitigation strategies, organisations need to identify their assets and perform a risk assessment to identify the level of protection required from various cyber threats. Furthermore, organisations require motivation to improve their cyber security posture, supportive executives, access to skilled cyber security professionals and adequate financial resources. Motivators can include a significant 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.

The following page provides 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.

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.

No set of mitigation strategies is guaranteed to prevent all cyber security incidents. However, properly implementing the eight mitigation strategies with an ‘essential’ effectiveness rating is so effective at mitigating targeted cyber intrusions and ransomware, that the ACSC considers these to be the new cyber security baseline for all organisations.

The companion Strategies to Mitigate Cyber Security Incidents – Mitigation Details publication contains implementation guidance for the mitigation strategies, as well as guidance to mitigate ‘business email compromise’ and threats to Industrial Control Systems. Further, the companion Essential Eight Maturity Model publication advises how to implement mitigation strategies in a phased approach and how to measure the maturity of their implementation. Finally, the ACSC’s website has supporting guidance in the Information Security Manual, as well as separate guidance for mitigating denial of service, and securely using cloud computing and enterprise mobility.
Strategies to Mitigate Cyber Security Incidents

Suggested Mitigation Strategy Implementation Order

1. Implement ‘essential’ mitigation strategies to:
   a. recover data and system availability
   b. limit the extent of cyber security incidents
   c. detect cyber security incidents and respond
   d. Repeat step 1 with ‘excellent’ mitigation strategies.
   2. Repeat step 1 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. limit the extent of cyber security incidents
   d. detect cyber security incidents and respond
   2. Repeat step 1 with ‘excellent’ mitigation strategies.
   3. Repeat step 1 with less effective mitigation strategies until an acceptable level of residual risk is reached.

Note that ‘hunt to discover incidents’ is less relevant for ransomware that immediately makes itself visible.

Malicious insiders who steal data:

1. Implement ‘essential’ mitigation strategies to:
   a. recover data and system availability
   b. prevent malware delivery and execution
   c. limit the extent of cyber security incidents
   2. Repeat step 1 with ‘excellent’ mitigation strategies.
   3. Repeat step 1 with less effective mitigation strategies until an acceptable level of residual risk is reached.

Malicious insiders who destroy data and prevent computers/networks from functioning:

1. Implement ‘essential’ mitigation strategies to:
   a. recover data and system availability
   b. limit the extent of cyber security incidents
   c. detect cyber security incidents and respond
   d. Repeat step 1 with ‘excellent’ mitigation strategies.
   2. Repeat step 1 with less effective mitigation strategies until an acceptable level of residual risk is reached.

Mitigation Strategies to Prevent Malware Delivery and Execution:

<table>
<thead>
<tr>
<th>Mitigation Strategy</th>
<th>Potential User Resistance</th>
<th>Uphornt Cost (staff, software and hardware)</th>
<th>Ongoing Maintenance Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Essential</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>Essential</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Essential</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>

Mitigation Strategies to Limit the Extent of Cyber Security Incidents:

<table>
<thead>
<tr>
<th>Mitigation Strategy</th>
<th>Potential User Resistance</th>
<th>Uphornt Cost (staff, software and hardware)</th>
<th>Ongoing Maintenance Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Essential</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>Essential</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Essential</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>

Mitigation Strategies to Detect Cyber Security Incidents and Respond:

<table>
<thead>
<tr>
<th>Mitigation Strategy</th>
<th>Potential User Resistance</th>
<th>Uphornt Cost (staff, software and hardware)</th>
<th>Ongoing Maintenance Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Excellent</td>
<td>Very High</td>
<td>Very High</td>
<td>Very High</td>
</tr>
<tr>
<td>Excellent</td>
<td>Very High</td>
<td>Very High</td>
<td>Very High</td>
</tr>
</tbody>
</table>

Mitigation Strategies to Recover Data and System Availability:

<table>
<thead>
<tr>
<th>Mitigation Strategy</th>
<th>Potential User Resistance</th>
<th>Uphornt Cost (staff, software and hardware)</th>
<th>Ongoing Maintenance Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Essential</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>Essential</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Essential</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>

Mitigation Strategies Specific to Preventing Malicious Insiders:

<table>
<thead>
<tr>
<th>Mitigation Strategy</th>
<th>Potential User Resistance</th>
<th>Uphornt Cost (staff, software and hardware)</th>
<th>Ongoing Maintenance Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very Good</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>
Summary of key changes since previous version

The title and scope of the publication 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 Mitigation Details publication has new guidance for these threats as well as for business email compromise and industrial control systems.

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.

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.

Effectiveness ratings now include ‘very good’, while ‘average’ has been changed to ‘limited’.

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

The two patching mitigation strategies now reference the ACSC’s definition of ‘extreme risk’ security vulnerabilities to reflect that the 48 hour (previously two day) timeframe to apply patches doesn’t apply to every security 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.

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. The ACSC has seen our guidance mitigate attempts to compromise Australian organisations by adversaries working for a foreign intelligence service.

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.

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.

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

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. Details are in the Mitigation Details publication.

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.

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

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’.

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

If you have any questions regarding this guidance you can [write to us](https://cyber.gov.au) or call us on 1300 CYBER1 (1300 292 371).