Australian Government
Australian Signals Directorate

# Strategies to mitigate cyber security incidents

**First published:** February 2010
**Last updated:** February 2017

## Introduction

The Australian Signals Directorate (ASD) has developed prioritised mitigation strategies to help 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 ASD'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 ASD 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, ASD's cyber.gov.au 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

**Last Updated: February 2017. First published February 2010.**

**Suggested Mitigation Strategy Implementation Order**
(start with threats of most concern to the organisation)

**Targeted cyber intrusions** (advanced persistent threats) and other external adversaries who steal data:

1. Implement 'essential' 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 'excellent' mitigation strategies.
3. 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 'Control removable storage media and connected devices' to mitigate data exfiltration.
2. Implement 'Outbound web and email data loss prevention'.
3. Implement 'essential' mitigation strategies to:
   a. limit the extent of cyber security incidents
   b. detect cyber security incidents and respond.
4. Repeat step 3 with 'excellent' mitigation strategies.
5. Implement 'Personnel management'.
6. If employees are likely to have hacking skills and tools, implement 'essential' mitigation strategies to prevent malware delivery and execution, and repeat step 3 with less effective mitigation strategies until an acceptable level of residual risk is reached.

Note that technical mitigation strategies provide incomplete security since data could be photographed or otherwise copied from computer screens or printouts, or memorised and written down outside of the workplace.

---

**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.
2. Repeat step 1 with 'excellent' mitigation strategies.
3. Implement 'Personnel management'.
4. If employees are likely to have hacking skills and tools, implement 'essential' mitigation strategies to prevent malware delivery and execution, and repeat step 1 with less effective mitigation strategies until an acceptable level of residual risk is reached.

| Relative Security Effectiveness | 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' 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 |
| **Mitigation strategies to limit the extent of cyber security incidents:** | | | | |
| Essential | **Restrict administrative privileges** to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Don't use privileged accounts for reading email and web browsing. | 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. | Low | Medium | Medium |
| Essential | **Multi-factor authentication** including for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive/high-availability) data repository. | Medium | High | Medium |
| Excellent | **Disable local administrator accounts** or assign passphrases that are random and unique for each computer's local administrator account to prevent propagation using shared local administrator credentials. | Low | Medium | Low |
| Excellent | **Network segmentation**. Deny traffic between computers unless required. Constrain devices with low assurance (e.g. BYOD and IoT). Restrict access to network drives and data repositories based on user duties. | Low | High | Medium |
| Excellent | **Protect authentication credentials**. Remove CPassword values (MS14-025). Configure WDigest (KB2871997). Use Windows Defender Credential Guard. Change default passphrases. Require long complex passphrases. | Medium | Medium | Low |
| Very Good | **Non-persistent virtualised sandboxed environment**, denying access to important (sensitive/high-availability) data, for risky activities (e.g. web browsing, and viewing untrusted Microsoft Office and PDF files). | Medium | Medium | Medium |
| Very Good | **Software-based application firewall, blocking incoming network traffic** that is malicious/unauthorised, and denying network traffic by default (e.g. unneeded/unauthorised RDP and SMB/NetBIOS traffic). | Low | Medium | Medium |
| Very Good | **Software-based application firewall, blocking outgoing network traffic** that is not generated by approved/trusted programs, and denying network traffic by default. | Medium | Medium | Medium |
| Very Good | **Outbound web and email data loss prevention**. Block unapproved cloud computing services. Log recipient, size and frequency of outbound emails. Block and log emails with sensitive words or data patterns. | Medium | Medium | Medium |
| **Mitigation strategies to detect cyber security incidents and respond:** | | | | |
| Excellent | **Continuous incident detection and response** with automated immediate analysis of centralised time-synchronised logs of allowed and denied computer events, authentication, file access and network activity. | Low | Very High | Very High |
| Very Good | **Host-based intrusion detection/prevention system** to identify anomalous behaviour during program execution (e.g. process injection, keystroke logging, driver loading and persistence). | Low | Medium | Medium |
| Very Good | **Endpoint detection and response software** on all computers to centrally log system behaviour and facilitate cyber security incident response activities. Microsoft's free SysMon tool is an entry level option. | Low | Medium | Medium |
| Very Good | **Hunt to discover incidents** based on knowledge of adversary tradecraft. Leverage threat intelligence consisting of analysed threat data with context enabling mitigating action, not just indicators of compromise. | Low | Very High | Very High |
| Limited | **Network-based intrusion detection/prevention system** using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries. | Low | High | Medium |
| Limited | **Capture network traffic** to and from corporate computers storing important data or considered as critical assets, and network traffic traversing the network perimeter, to perform incident detection and analysis. | Low | High | Medium |
| **Mitigation strategies to recover data and system availability:** | | | | |
| Essential | **Regular backups** of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes. | Low | High | High |
| Very Good | **Business continuity and disaster recovery plans** which are tested, documented and printed in hardcopy with a softcopy stored offline. Focus on the highest priority systems and data to recover. | Low | High | Medium |
| Very Good | **System recovery capabilities** e.g. virtualisation with snapshot backups, remotely installing operating systems and applications on computers, approved enterprise mobility, and onsite vendor support contracts. | Low | High | Medium |
| **Mitigation strategy specific to preventing malicious insiders:** | | | | |
| Very Good | **Personnel management** e.g. ongoing vetting especially for users with privileged access, immediately disable all accounts of departing users, and remind users of their security obligations and penalties. | High | High | High |

# 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 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.

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 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 or call us on 1300 CYBER1 (1300 292 371).