FEBRUARY 2017

Strategies to Mitigate Cyber Security Incidents

(replaces the document Strategies to Mitigate Targeted Cyber Intrusions)

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.

Strategies to Mitigate Cyber Security Incidents

UPDATED FEBRUARY 2017
First published February 2010

Suggested Mitigation Strategy Implementation Order
(start with the 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 Rating	Mitigation Strategy	Potential User Resistance	Upfront Cost (staff, equipment, technical complexity)	Ongoing Maintenance Cost (mainly staff)
Mitigation Strategies to Prevent Malware Delivery and Execution:				
Essential	**Application whitelisting** of approved/trusted programs 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"[1] 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**. Whitelist allowed 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**. Whitelist allowed 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 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"[1] 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 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 permitted and denied: computer events, authentication, file access, 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 incident response. 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	**Daily 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 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.

[1] http://www.asd.gov.au/publications/protect/assessing_security_vulnerabilities_and_patches.htm