Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Managing the risks of legacy IT: Practitioner guidance

First published: April 2024
Last updated: June 2024

Introduction

Legacy information technology (IT) presents significant and enduring risks to the cyber security posture of Australian Government entities and organisations. Its presence can increase the risk of a cyber security incident, and make any cyber security incident that does occur much more impactful.

This publication provides guidance for organisations on mitigating the risks posed by legacy IT within their IT environments. It also sets out low-cost mitigations for legacy IT that organisations can draw upon, in addition to their own strategies. Although, the mitigations suggested in this document provide only temporary risk reduction.

While this guidance is primarily intended for Australian Government entities, it can be used by any organisation to manage the risks of legacy IT within their IT environments.

The most effective method to mitigate the risk posed by legacy IT is to replace it before it becomes legacy. Retaining legacy IT within an organisation's IT environment, especially where adequate mitigations have not been applied, also presents significant business risks. These include the costs involved in remediating the consequences following a cyber security incident, systems being taken offline, service delivery being disrupted, loss of productivity, potential leakage or loss of data, and loss of public confidence.

This guidance should be read in conjunction with other guidance from the Australian Signals Directorate (ASD), including:

- *End of support for Microsoft Windows and Microsoft Windows Server*
- *Gateway security guidance package: Gateway operations and management*
- *Hardening Microsoft 365, Office 2021, Office 2019 and Office 2016*
- *Implementing multi-factor authentication*
- *Information security manual*
- *Mergers, acquisitions and Machinery of Government changes*.

Defining legacy IT

Under the Department of Home Affairs' *Protective Security Policy Framework*, an IT product (i.e. hardware, software, services, protocols and/or systems) is considered to be legacy when it meets one or more criteria from both Category A and Category B below.

Category A

- considered an end-of-life product, or
- out of support, and extended support from the manufacturer, vendor or developer.

Category B

- impractical to update or support within the entity, or
- no longer cost-effective, or
- considered to be above the current acceptable risk threshold, or
- offers diminishing business utility, or
- prevents or obstructs fulfilment of the entity's IT strategies.

Detailed examples of IT that would meet these criteria, or be considered legacy, are provided in the Department of Home Affairs' *Protective Security Policy Framework*.

Managing legacy throughout the lifecycle of IT

All IT will eventually become legacy and present acute security risks. Therefore, organisations cannot afford to avoid planning for the depreciation of their IT.

All organisations should strive to implement a clear strategy for managing legacy IT now and into the future. Organisations should consider the high-level principles below when formulating their legacy IT management strategy. Foresight and frontloaded investment will allow organisations to reduce business and security risks, and avoid significant future costs.

Facilitate good communication with stakeholders

One of the biggest hurdles that IT teams can face when mitigating the risks associated with legacy IT is the reluctance of business units to replace legacy IT or implement business-limiting mitigations. For example, IT teams may encounter business units that prioritise availability over the security of systems.

When looking to replace legacy IT, it is important that IT teams keep business owners informed of the potential impacts of legacy IT. IT teams should articulate the risks presented by legacy IT in terms of potential impact to service delivery, business continuity, lost productivity and loss of public confidence. Replacing or mitigating legacy IT early is likely to have less impact on productivity than replacing legacy IT in response to a cyber security incident.

While legacy IT can pose a significant and enduring risk in isolation, the risk posed by legacy IT in aggregate is significantly higher. Chief information security officers should also be aware of the risk that legacy IT poses in aggregate and regularly convey the aggregate risk of legacy IT to business and management structures.

Know your IT environment

A key element of a sound strategy for managing legacy IT within organisations is having a complete picture of the IT environment through an accurate IT register. Developing, implementing and maintaining an accurate IT register can

be a significant undertaking but is essential to managing the risks of legacy IT. If possible, develop a Software Bill of Materials to support the IT register.

It is also essential to understand what dependencies legacy IT relies upon to stay supported. While IT typically relies on external vendor, manufacturer or developer support, organisations should also consider internal dependencies. For example, IT that is supported by internal staff may depreciate to legacy status when staff with the requisite skills to maintain that IT leave the organisation.

Plan for future depreciation as part of procurement

All IT will eventually become legacy and need to be replaced. When organisations procure IT, they should consider these as 'whole-of-life costs', as per the *Commonwealth Procurement Rules*.

Organisations need to consider the skilled human resources, technical controls and other processes that will be required to manage IT depreciation into legacy status in the future. Early consideration of the depreciation of IT can also reduce transition costs and periods of downtime when legacy IT systems are replaced. This is explored further in the Digital Transformation Agency's *Digital Lifecycle Considerations*.

For some Australian Government entities, this requirement is reinforced by the PSPF that requires Non-Corporate Commonwealth Entities to '…ensure the secure operation of their ICT systems…during all stages of the lifecycle of each system', which includes the 'define' and 'design' stages of systems' lifecycle.

Continuously monitor depreciation across your IT environment

Vendors, manufacturers and developers of IT – whether internal or external – often give advance notice of when their product will reach end-of-life or out-of-support status. Organisations should be attentive to these communications, which will assist with forward planning for the product's replacement or upgrade.

In addition to these ad hoc responses, organisations should consider instituting a policy or process for systematically monitoring when their IT will depreciate, or whether they have already depreciated, into legacy status. Organisations should plan to conduct IT environment-wide reviews on a realistic and regular cadence. Implementing this policy and process will leverage the work to develop an accurate IT register. Further, systemically monitoring for newly or soon-to-be depreciated IT enables organisations to understand the risk posed by legacy IT in aggregate.

As part of monitoring for the depreciation of IT across the IT environment, organisations should monitor whether staff that are essential to preventing the depreciation of IT into legacy status are still present and available in the organisation. This is also important to monitor when organisations undergo mergers, either through Machinery of Government changes or a merger and acquisition in the private sector – noting that organisations may lose expertise or resources required to support legacy IT that it had access to prior to that merger.

Replace legacy IT

The most effective way to mitigate the risks associated with legacy IT is to replace it with IT that is still in support. For legacy IT that has many interdependencies, or is embedded in business processes, it may be appropriate to replace it incrementally. A phased approach can spread out costs and potentially reduce the business impact and limit risk.

The longer legacy IT remains in organisations' environments, the harder it will become to find staff with the technical skills to operate and support it. It may also become more embedded in business processes or more difficult to replace as time goes on.

Replacement of legacy IT can be expensive and logistically complex, especially when it has not been considered early in the procurement lifecycle. Delaying replacement, however, may only compound these costs and technical challenges in future.

When you cannot replace legacy IT apply temporary mitigations

The existence of legacy IT in organisations' environments will always result in the presence of business and security risk. If replacement of legacy IT is not yet feasible, or will take time to achieve, organisations should apply temporary mitigations.

The following list provides ASD's recommended mitigations that organisations can apply to the risks associated with legacy IT. This list is not exhaustive and organisations may consider implementing their own mitigations that are more relevant to their IT environments. These mitigations are not long-term solutions. The only long-term solution is the replacement of legacy IT.

Implement appropriate network segmentation and/or segregation

Network segmentation and segregation are the most effective controls in preventing malicious actors from easily propagating throughout networks once they gain initial access. To achieve appropriate segmentation and/or segregation, networks can be segregated into multiple network zones in order to protect servers, services and data.

Network segmentation uses existing or additional routers and firewalls to isolate legacy IT in one or more network segments. This will restrict broader network access to the rest of the IT environment from a compromised legacy host. Some specific applications of network segmentation include:

- Organisations should restrict the exposure of legacy IT to the internet by internalising any external facing websites or services that have no need to be external facing. Doing so denies a significant number of attack vectors for legacy IT.

- The use of cloud or on premise emulation services can provide inherent network segmentation and segregation. Running applications that require a legacy operating system (OS) within virtual environments enables the OS to run cocooned within modern software with increased logging, detection and prevention capabilities.

See *Guidelines for networking*.

Implement common hardening techniques

Hardening advice, such as those contained within the *Guidelines for system hardening*, should be applied to legacy IT. Hardening advice can include the removal of default accounts or credentials, restricting the abilities of unprivileged users, and stopping unnecessary services. Applying common hardening techniques can prevent common threat vectors such as privilege escalation and default account exploitation. Some key hardening considerations include:

- Do not deploy a legacy OS in its default state. Doing so can lead to an insecure operating environment that may allow malicious actors to gain an initial foothold on a network. OS settings can be configured to mitigate security risk through the use of ASD and vendor hardening guidance.

- Disable unused services on systems. The more services that a system runs, the higher likelihood that one of those services will have an exploitable vulnerability that can compromise the whole system. Therefore, a system should only run the minimum number of services required. Common unused services that are often running by default include the Print Spooler, fax services and Bluetooth.

- Close unused ports on systems. Ports enable connections between systems but not all ports are required by a system. Only the required reports should be open, with all other ports closed. This approach can be enforced at

two levels, the system level and the network level. Specifically, system level port restriction should use network communication capabilities of the system itself to block the ports, or software tools such as a host-based firewall, while network level port restriction should be is enabled through network routing information or firewall enforcement. Network segmentation restricts not only IP-level connections but also port connections, therefore, approved IP addresses can only connect through approved ports or protocols.

- Apply hardening guidance from ASD and vendors to applications. While some vendors may not provide updates for their legacy applications, most vendors provide guides on the best way to harden them by disabling features and/or configuring settings. This vendor guidance is often designed to show how certain configurations reduce the attack surface of applications.

See *Guidelines for system hardening* and *Guidelines for information technology equipment*.

Implement multi-factor authentication and account hygiene

Multi-factor authentication is often used to stop malicious actors from easily compromising accounts. If implementing multi-factor authentication for a legacy host is not possible, consider implementing it on the boundary of a segmented system. For example, when IT does not support multi-factor authentication, enable multi-factor authentication as part of the jump server authentication process and conduct all administration via the jump server.

In addition to implementing multi-factor authentication, implement and regularly undertake account hygiene practises, such as restricting user access to legacy IT (to the greatest extent possible) while removing old and/or unused accounts. Proper account hygiene also includes the scheduled revalidation or approval of accounts, especially for users with privileged access.

Basic account hygiene is key to reducing multiple threat vectors in an IT environment. For example, if during the development of an application a set of usernames and passwords were created for testing purposes, then these accounts should be removed prior to release of the application into production.

See *Implementing multi-factor authentication* and *Guidelines for system hardening*.

Enable or increase logging and monitoring of legacy IT

Increasing logging and monitoring of legacy IT can enable the detection of malicious actors before they disperse across the IT environment. Logging within legacy IT is often difficult due to reduced capacity for log generation and storage. Where possible, log to a centralised logging location and log access to supporting jump servers and intermediate hosts. For those with Microsoft Windows environments, consider the use of the Cybersecurity and Infrastructure Security Agency's free Logging Made Easy toolkit available on GitHub.

Concurrent to logging, review legacy applications for information leakage. Information leakage occurs when the default error page of legacy applications displays sensitive data, such as the Java version used. This data equips malicious actors with information that can be used to compromise a system. Where possible, remove the presence of sensitive data by customising the default error pages to restrict this data or display a more benign message instead of detailed system information.

See *Guidelines for security assurance*, *Implementing multi-factor authentication* and *Guidelines for system hardening*.

Implement application attack surface reduction

Applications present a risk when they contain configuration weaknesses that malicious actors can exploit. By removing configuration weaknesses, or otherwise minimising the capabilities and functionality of an application, organisations can reduce this threat vector. File Type Blocking can be used to further reduce the attack surface by blocking insecure file types such as legacy, binary and beta file types from opening in Microsoft Office.

A key business application used by many organisations is a web browser. The use of legacy web browsers, such as Internet Explorer 11, often in combination with other legacy IT such as protocols supporting outdated encryption algorithms, introduce significant risks. These legacy web browsers often have significant vulnerabilities without no remediation support from vendors.

See *Guidelines for system hardening* and *Hardening Microsoft 365, Office 2021, Office 2019 and Office 2016*.

Schedule system availability and access

Legacy IT required for periodic events should only be powered on while in use and then shut off. While active, additional logging and monitoring should occur to ensure that the system's integrity is maintained. There is an element of risk with this mitigation if, in addition to obsolete software, the hardware is considered legacy and may not restart. Organisations should consider the hardware status prior to committing to this mitigation.

If a specific application is only required for discrete periods, then shut down or close the application when not in use to prevent unauthorised access. Configure access periods to known activity times to provide windows of access to the legacy IT.

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).

Appendix A: Suggested implementation

Category	Mitigation Strategy	Implementation Difficulty	Implementation Cost	User Impact	Maintenance Cost	Hypothetical Example
Operating Systems For example, old and unsupported versions of Microsoft Windows and Linux.	Implement appropriate network segmentation and/or segregation	Medium	Low	Low	Low	A legacy Microsoft Windows Server 2003 host is discovered on an Active Directory domain. The organisation has noted that there is a project to decommission this server, but resourcing is yet to be allocated for a replacement. To help mitigate the risks in the interim, the organisation decides to implement network segmentation to restrict access to the system, review and restrict the accounts with access to the system to a controlled subset, disable unused services and ports on the server, and increase the monitoring for the system.
	Implement common hardening techniques	Medium	Medium	Low	Low	
	Implement multi-factor authentication and account hygiene	Low	Medium	Low	Low	
	Enable or increase logging and monitoring of legacy IT	Low	Medium	Low	Low	
	Schedule system availability and access	Low	Low	Medium	Low	
Applications For example, software that is no longer supported by the vendor or in-house developed tools without appropriate resourcing for ongoing support or upgrades.	Implement appropriate network segmentation and/or segregation	Medium	Low	Low	Low	An internally developed application transitions to legacy status as there is no longer ongoing support for it. The application is only required on a quarterly basis to complete tasks. The organisation decides to harden the underlying server the application resides on, review the application for information leakage and ensure the application is shutdown between periods of demand.
	Implement common hardening techniques	Medium	Medium	Low	Low	
	Implement multi-factor authentication and account hygiene	Low	Medium	Low	Low	
	Enable or increase logging and monitoring of legacy IT	Low	Medium	Low	Low	
	Implement application attack surface reduction	Medium	Medium	Low	Low	
	Schedule system availability and access	Low	Low	Medium	Low	
Infrastructure For example, webservers, Active Directory domains, and protocols that are out of support.	Implement common hardening techniques	Medium	Medium	Low	Low	A webserver hosting a legacy website is accessible on the external-facing internet. The organisation decides to mitigate the risk this presents by internalising the website so that it is no longer available on the internet, and reviews the site for opportunities to mitigate information leakage.
	Implement multi-factor authentication and account hygiene	Low	Medium	Low	Low	
	Enable or increase logging and monitoring of legacy IT	Low	Medium	Low	Low	
Hardware devices For example, routers, switches and security cameras.	Implement appropriate network segmentation and/or segregation	Medium	Low	Low	Low	A legacy security camera system is required to operate in a priority site. The organisation could review the users that have access to the system, and implement network controls to ensure segregation between the legacy system and corporate networks.
	Implement multi-factor authentication and account hygiene	Low	Medium	Low	Low	
	Enable or increase logging and monitoring of legacy IT	Low	Medium	Low	Low	

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

© Commonwealth of Australia 2024.

With the exception of the Coat of Arms, the Australian Signals Directorate logo and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International licence (www.creativecommons.org/licenses).

For the avoidance of doubt, this means this licence only applies to material as set out in this document.

The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 licence (www.creativecommons.org/licenses).

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (www.pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines).

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government

Australian Signals Directorate