Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Managing the risks of legacy IT: Executive guidance

First published: April 2024
Last updated: June 2024

Introduction

This publication summarises the meaning of 'legacy' information technology (IT), why it is important to manage the risks associated with it and how to empower IT teams to manage it.

While this guidance is primarily intended for Australian Government executives, it can be used by any organisation in managing the risks of legacy IT.

What is 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.

Why is legacy IT so risky?

Security updates protect against cybersecurity incidents by adding new security features and fixing software bugs (i.e. coding errors or vulnerabilities). As legacy IT does not receive security updates, it is more vulnerable to cyberattacks.

Malicious actors may not only be able to compromise legacy IT in your IT environment, but also use it to gain access to more modern systems that your organisation relies on. Keeping legacy IT in your IT environment therefore increases the risk that your organisation will experience a cybersecurity incident. It can also make any cybersecurity incident that does occur much more impactful.

There are also significant business risks associated with legacy IT in your IT environment. For example, legacy IT can increase the likelihood that your organisation will have systems taken offline, service delivery disrupted, data destroyed or leaked, and public confidence lost. Furthermore, remediating a cybersecurity incident involving legacy IT, and managing its consequences, may also involve high financial costs. It is always less costly to mitigate the risks of legacy IT before a major cybersecurity incident occurs.

Finally, retaining legacy IT in your IT environment is a significant and enduring risk to your organisation and its operations, with the risks posed compounded when multiple forms of legacy IT are present. As such, your organisation should consider the risk posed by legacy IT in aggregate as well as in isolation. Chief information security officers should convey these risks to business groups and corporate risk management processes.

Case study: Legacy IT leads to ransomware incident in a NSW council

In April 2022, malicious actors exploited a legacy IT entry point in a New South Wales local council's IT environment to gain access to its network. The entry point was no longer receiving support from its vendor and the council did not have the ability to maintain the entry point itself. After entering the network through the entry point, the malicious actors deployed ransomware and encrypted the council's minutes, employee financial data and water quality monitoring systems.

The council's IT staff worked between 40-80 hours of overtime that week while responding to the ransomware incident. The council also had to pay for the services of a commercial cybersecurity incident response provider, and engage its managed service provider to regain access to its systems. Water quality had to be manually monitored in the weeks following the ransomware incident, expending significant resources.

The council incurred significant cost in responding to the ransomware incident that it could have avoided had it invested the resources necessary to mitigate the risks associated with its legacy IT.

What does it take to manage the risks?

Implementing a sound strategy to manage legacy IT in your IT environment will likely require upfront costs and resources. However, establishing a strategy that allows your organisation to plan for the depreciation of IT into legacy status is likely to avoid more significant costs in the future.

Legacy IT becomes more difficult and expensive to replace over time, as the technical skills needed to manage it become rarer and it becomes further embedded in business processes. Replacing legacy IT in your IT environment may become harder when staff with the technical skills to support your legacy IT leave your organisation.

All IT your organisation uses will become legacy IT at some point and present acute security risks. Consequently, these risks need to be continuously managed as your existing IT ages and new IT is procured. Longer term, it is easier to plan for future depreciation of IT into legacy status as part of procurement. This will require proactive consideration of the costs in decommissioning, replacing or applying mitigations to all IT in the future.

The most effective strategy to eliminate the risks associated with legacy IT is to replace it with IT that is still receiving support – whether that support is internal or external. Where this is not feasible, or replacing legacy IT will take time, temporary measures should be adopted to mitigate some of the risk.

Implementing a sound strategy to manage legacy IT requires:

- working with your cybersecurity team to understand the business and security risks posed by legacy IT – both in isolation and in aggregate
- developing an accurate register of all IT in your organisation, if there is not one already
- maintaining that IT register, and regularly monitoring your organisation's IT environment to ensure the IT is still vendor supported
- planning for the risks associated with legacy IT as part of procurement
- replacing legacy IT with IT that is still vendor supported
- applying temporary mitigations to legacy IT when replacement is not yet feasible.

While the above advice will not eliminate the risks of legacy IT, encouraging your IT staff to implement guidance from the supporting *Managing the risks of legacy IT: Practitioner guidance* publication can assist with further reducing some of the risks associated with legacy IT.

Further information

The *Information security manual* is a cybersecurity framework that organisations can apply to protect their systems and data from cyberthreats. The advice in the *Strategies to mitigate cybersecurity incidents*, along with its Essential Eight, complements this framework.

Contact details

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

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.

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

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

Australian Government

Australian Signals Directorate