Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Stakeholder kit

Legacy technology

Table of contents

About this kit

Don’t let legacy technology define your legacy

The Australian Signals Directorate’s Australian Cyber Security Centre (ASD’s ACSC) has identified 4 priority actions that are key to bolstering the cyber security of any organisation.

We are encouraging executive, business owners and IT and cyber security professionals to take action on the first of these priorities - legacy technology.

What is legacy technology and why is it a risk?

Legacy technology is outdated hardware and software that is no longer supported by the manufacturer, vendor or developer and cannot receive important security updates or patches.

From a cyber criminal’s point of view, legacy technology is an attractive target as it represents a low-resistance entry path into otherwise well-defended environments. Malicious actors can use vulnerabilities in legacy technology as an entry point to pivot into other more modern systems that your organisation relies on.

Replacing your legacy technology may be less expensive than a cyber attack. The average self-reported cost of cybercrime for businesses is $80,000. Can you afford that risk?

If you cannot update your legacy technology now or replacement will take time, adopt additional security measures to mitigate some of the risk. These measures include implementing or increasing event logging, network segmentation and/or segregation, system hardening, multi-factor authentication and account hygiene, application surface reduction and restricting system availability and access windows.

Visit cyber.gov.au/legacytech for more advice on legacy technology.

Tactics to consider

You can use the key messages and resources in this kit to raise awareness of ASD’s ACSC’s legacy technology advice and messaging, by:

- ✓ Telling your technical audiences, stakeholders, staff and customers about the importance of updating legacy technology and share the key messages.
- ✓ Featuring content and information about legacy technology in internal and external newsletters and on your website.
- ✓ Forwarding to your communications team to repurpose this content across your internal and external communications channels.
- ✓ Sharing content from this kit on social media and encourage the audience to take action.
- ✓ Providing talking points to your managers, senior leaders and executive for meetings, events and engagements to start the conversation about cyber security.
- ✓ Directing people to cyber.gov.au/legacytech to learn how to take action on legacy technology.

Key messages

General messages

- Legacy technology does not receive security updates and can leave you more vulnerable to cyber attacks.
- The average self-reported cost of cybercrime for businesses is more than $80,000. Can you afford a cyber attack?
- Replacing legacy technology can be cheaper than a major cyber incident.
- Old tech lets threats thrive.
- Boost your cyber security by isolating your vulnerable systems from critical assets.
- Don’t let legacy technology define your legacy.
- Keeping old technology is not economical. It is a threat and may end up costing you more.
- Legacy technology is any technology that is no longer supported by the vendor or developer.
- When is the last time you updated or replaced your technology?
- Is your technology ready for retirement?

Calls to action

1. Retire your legacy technology now. Visit cyber.gov.au/legacytech
2. Can’t retire legacy technology? This is what to do. Visit cyber.gov.au/legacytech
3. Update or replace your legacy technology now. Read cyber.gov.au/legacytech
4. Take action now. Learn more at cyber.gov.au/legacytech
5. What if you can’t update now?

If you can’t afford to update now or updating will take some time, it’s important to adopt additional security measures to mitigate some of the risk.

These 6 measures include implementing or increasing:

1. Best practice event logging
2. Appropriate network segmentation and/or segregation
3. Common hardening techniques
4. MFA and account hygiene
5. Application surface reduction
6. Scheduling system availability and access.

Editorial content

Use this suggested content across your communication channels, including newsletters, staff intranet pages, website news or blog articles, and customer or stakeholder emails.

Don’t let legacy technology define your legacy

Take action to ensure your legacy technology isn’t a threat to your organisation.

The Australian Signals Directorate’s Australian Cyber Security Centre (ASD’s ACSC) is encouraging organisations to take action on their legacy technology.

Legacy technology includes any technology no longer supported by the vendor, manufacturer or developer. Because of this, it does not receive the security updates or bug fixes necessary to protect against cyber incidents, making it more vulnerable to attack.

Malicious actors can use your legacy technology as an entry point to pivot into other more modern systems that your organisation relies on.

The most effective strategy to reduce the risk from legacy technology is to take action and replace it.

If replacement isn’t feasible, or may take time, adopt temporary measures like network segmentation and advanced logging and monitoring to reduce the associated risks.

Learn how to take action on legacy technology now at cyber.gov.au/legacytech

Social media posts

Use the suggested post text and links below on your social media channels. Feel free to adapt or tailor these messages to your audience and channels.

Platform	Purpose	Suggested post text
Facebook, Instagram and LinkedIn	Raise awareness/educate	Using legacy technology in your organisation may end up costing you more. Legacy technology is any technology no longer supported by the vendor, developer or manufacturer. Because of this, legacy technology does not receive the security updates or bug fixes necessary to protect against cyber incidents, making it more vulnerable to attack. The average self-reported cost of cybercrime for businesses is more than $80,000. Can you afford a cyber attack? Take action on your legacy technology at ☞ cyber.gov.au/legacytech
X (Twitter)	Raise awareness/educate	Old technology lets cyber threats thrive. Replacing legacy technology now is a vital mitigation to avoid expensive cyber attacks. Learn how to take action on your legacy technology at ☞ cyber.gov.au/legacytech

Get social

Join the conversation by following ASD's social media channels and share the latest cyber security social content with your followers. By sharing ASD's social content, you can help your followers improve their cyber security.

@ASDGovAU

Australian Signals Directorate

asd.gov.au

Australian Signals Directorate

Further resources

Become an ASD Partner

Want priority access to the latest resources and advice?

Join ASD's free Cyber Security Partnership Program as a Business Partner or Network Partner to receive cyber security alerts, advisories and up-to-date advice, as well as join initiatives to uplift the cyber resilience of Australian organisations.

Responding to cyber incidents

For immediate assistance during a cyber incident, **call the 24/7 Australian Cyber Security Hotline on 1300 CYBER1 (1300 292 371).**

ASD is not a regulator; we are here to help you respond to and recover from cyber incidents. Make sure to report cyber threats, incidents and vulnerabilities early and often at cyber.gov.au/report or call our 24/7 hotline.

If you request support, we can provide you with immediate advice and assistance, which may include:

1. information on how to contain and remediate an incident
2. intelligence and advisory products to help you with your incident response
3. linking you to Australian Government entities that may further support your response.

Every report helps us build a national cyber threat picture and informs the development of our advice and guidance.

About ASD's ACSC

The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) is the Australian Government's technical authority on cyber security.

Who we help

Our advice and assistance is for the whole economy, including:

- critical infrastructure and systems of national significance
- federal, state and local government
- small and medium businesses
- academia
- charities and not-for-profit organisations
- the Australian community.

What we do

ASD brings together capabilities to improve Australia's national cyber resilience. Its services include:

- providing the Australian Cyber Security Hotline, which is contactable 24 hours a day, 7 days a week, on 1300 CYBER1 (1300 292 371)
- publishing alerts, technical advice, advisories and notifications on significant cyber security threats
- monitoring cyber threats and intelligence sharing with partners
- helping Australian entities respond to cyber security incidents
- enhancing the cyber security resilience of Australian entities with exercises and uplift activities
- enabling Australian organisations and individuals to engage with the ASD's ACSC and fellow partners through ASD's Cyber Security Partnership Program.

The most effective cyber security is collaborative and our partnerships are key. We thank contributors to the development of our guidance and the organisations who help uplift Australia's cyber security by sharing the latest cyber security advice, alerts and guidance.

Further assistance

ASD is not a regulator; we are here to help you recover from cyber incidents. Make sure to report cyber threats, incidents and vulnerabilities early and often at cyber.gov.au/report or call 1300 292 371 (1300 CYBER1).

Your report helps us build a national cyber threat picture and informs the development of our advice and guidance.

Get in touch

If you would like to subscribe to receive future stakeholder kits from ASD's ACSC or have any questions, please email our Public Communication team at asd.publiccomms@defence.gov.au.

Australian Government

Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre