Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Stakeholder kit

Cyber supply chain risk

Contents

About this kit

One breach can break the chain

The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) has identified 4 priority actions — replace legacy technology, implement best practice event logging, manage supply chain risk and prepare for quantum cryptography — which are key to bolstering the cyber security of any organisation.

This month, we are encouraging executives, business owners and IT and cyber security professionals to take action on cyber supply chain risk.

What is a cyber supply chain and what is the risk?

Every organisation relies on external suppliers, manufacturers, distributors, contractors or retailers to do business.

Not only is the cyber security of your organisation important, so too is the cyber security of your cyber supply chain. Malicious actors can gain access to your important networks and information through your cyber supply chain.

That's why it is vital to take action on cyber supply chain risk by:

- identifying the cyber supply chain
- understanding cyber supply chain risk
- setting cyber security expectations
- auditing for compliance
- monitoring and improving cyber supply chain security practices
- visiting cyber.gov.au/supplychain to learn how to mitigate cyber supply chain risk.

Tactics to consider

You can use the key messages and resources in this kit to raise awareness of ASD's ACSC's cyber supply chain risk advice by:

- Telling your technical audiences, stakeholders, staff and customers about the importance of mitigating cyber supply chain risk.
- Featuring content and information about cyber supply chain risk 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 your audiences to take action.
- Providing talking points to your managers, senior leaders and executive for meetings, events and engagements to start conversations about cyber supply chain risk.
- Directing people to cyber.gov.au/supplychain to learn how to take action on you cyber supply chain.

Key messages

General messages

- One breach can break the chain. Protect your cyber supply chain.
- Identify, understand and audit your cyber supply chain. You are only as strong as your weakest link.
- Weak cyber supply chains can allow malicious actors access to your networks and data.
- The cyber security vulnerabilities of your suppliers are also your vulnerabilities.
- Distributors, contractors, suppliers, manufacturers and retailers all play a role in keeping your information and networks safe.
- Take action to boost your supply chain's cyber security.

Calls to action

- Secure your cyber supply chains now.
- Identify and take action on cyber supply chain risk.
- Learn more: cyber.gov.au/supplychain

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.

Your cyber supply chain is only as strong as your weakest link

Identify, understand and audit your cyber supply chain today.

The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) is encouraging organisations to understand and take action on their cyber supply chain risk.

Cyber supply chain risk refers to vulnerabilities introduced by any third party that touches your products or services, meaning weaknesses can emerge at any point. From suppliers and manufacturers to distributors, retailers or contractors, each of these partners handles systems, components or data you rely on. Any compromise in their environment can directly become a compromise in yours.

Cyber supply chain risk management should form a significant component of any organisation's overall cyber security strategy, and you must treat the security of your cyber supply chain as seriously as your own.

There are strategies you can implement to mitigate supply chain risk and protect your organisation from cyber attacks.

Learn more at cyber.gov.au/supplychain

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	Have you ever considered the cyber security strength of your suppliers? Weak cyber supply chains can allow malicious actors to access your most important data and networks. Identify, understand and audit your cyber supply chain today. Learn more at ☞ cyber.gov.au/supplychain
X (Twitter)	Raise awareness/educate	Have you ever considered the cyber security strength of your suppliers? Your cyber security is only as strong as your cyber supply chain's weakest link. Learn how to take action on cyber supply chain risk at ☞ cyber.gov.au/supplychain

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