Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Australian Institute of Company Directors

Cyber security priorities for boards in 2025-26

First published: 30 October 2025

Introduction

The Australian Signals Directorate (ASD) prevents, disrupts and responds to attacks against Australian organisations every day. Understanding and managing cyber security risks, as with other business risks, is a key responsibility in protecting your organisation, shareholders and customers.

The Australian Institute of Company Directors (AICD) mission is to be the independent and trusted voice of governance, building the capability of a community of leaders for the benefit of Australian society. In recent years, the AICD has had a significant focus on educating directors on better practice cyber security and data governance through guidance and education activities.

Should we be worried about cyber security?

Today, Australia faces a heightened global cyber threat environment, driven by geopolitical tensions in the Middle East, Ukraine and the Indo-Pacific. Recent global events have shown that organisations must be prepared for state-based actors pre-positioning for disruptive attacks against critical infrastructure and services.

Australia has also endured a number of serious data breaches, compromising organisations and impacting customer trust, the cost of which cannot be understated. Unfortunately, trends are worsening. Malicious actors continue to target Australian organisations of all types and sizes. Espionage, enabled by technology advancements, cost Australia $12.5 billion in FY23–24. Cybercrime costs are also rising across all organisation types and sizes, with a sharp increase for large enterprises.

Where should the focus be in 2025-26?

Boards of directors (boards) play a critical role in overseeing how their organisations maintain and build cyber security capabilities, and in responding to existing and emerging cyber threats.

In 2025-26, we encourage a focus by boards on the following areas:

- Understanding whether technology used or provided to your customers is secure by design and secure by default. These security principles and practices are critical for building modern defensible architectures.
- Prioritising the defence of your organisation's most critical assets. Your organisations should operate with a mindset of 'assume compromise' and consider which assets or 'crown jewels' need the most protection.

Your organisation's ability to defend and respond can be further enhanced through implementing better practice event logging and threat detection measures, replacing legacy information technology (IT), effectively managing third-party risks, and beginning your post-quantum cryptography transition. However, we cannot forget, nor neglect, the basics. This includes keeping all devices updated and enabling multi-factor authentication, especially for any public-facing services. These heightened areas of focus are in addition to a board's core elements of effective cyber security, for instance, comprehensive cyber security incident planning and promoting a strong cyber security culture within their organisation.

What good cyber security governance look likes in 2025-26

The following advice outlines questions boards can ask of management and their organisation to understand its cyber security posture in the 2025-26 cyber threat environment. These questions should be read in conjunction with the AICD and the Cyber Security Cooperative Research Centre's *Cyber Security Governance Principles | Version 2* and *Governing Through a Cyber Crisis - Cyber Incident Response and Recovery for Australian Directors* publications. These publications provide an overview of the core principles of effective cyber security governance, including allocating roles and responsibilities and overseeing an effective cyber security strategy.

Taken together, the questions in this publication, and the AICD's cyber security governance guidance, represent a proactive approach to building cyber security capability in the current cyber threat environment.

The questions in this publication are divided into two categories:

- threshold governance questions that assist in determining the cyber security posture of organisations, given the 2025-26 cyber threat environment.
- supplementary technical questions to understand in greater detail the cyber security controls in place within organisations. These questions may assist directors of a risk or technology committee engage on key controls with senior management, by way of example.

We recognise that for many organisations, particularly small-to-medium enterprises and not-for-profits, it may not be possible to implement all the advice within this publication. However, this advice still enables the board for such entities to ask questions to understand their organisation's existing cyber security posture and identify areas for improvement.

ASD provides cyber security advice specifically written for small business at cyber.gov.au.

The AICD CSCRC Cyber Security Principles also has a dedicated snapshot for directors of smaller organisations.

Contact details

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

Does your organisation have event logging and threat detection?

The board should understand whether there is an enterprise wide-approach to event logging and threat detection. A rigorous approach to threat detection will improve your organisation's chances of detecting malicious behaviour within your IT environment.

In implementing cyber security measures, including event logging and threat detection measures, the board should have visibility of shared responsibilities between service providers and their organisation.

ASD provides advice for executives to assist with implementing event logging and threat detection.

Threshold governance questions

- Have we established an event logging policy that includes event log retention, access and review procedures?
- Have we defined event logging and monitoring responsibilities across teams?
- Have we identified all critical systems, applications and devices that require event logging?

Supplementary technical questions

Event logging processes and coverage

- Do our cyber security activities align with ASD's event logging and threat detection guidance?
- Do we collect event logs from network devices, security appliances, operating systems, applications, databases and cloud services?

Event log configuration and quality

- Do we configure event logs to capture sufficient detail?
- Do we ensure event logs are time-synchronised across our organisation?
- Do we avoid collecting excessive or irrelevant event logs?

Centralised event log management

- Do we forward event logs to a centralised event logging system?
- Do we ensure event logs are securely transmitted and stored?
- Do we implement access controls to protect the integrity and confidentiality of event logs?

Threat detection capabilities

- Do we define and implement detection rules for known cyber threats and anomalies?
- Do we use threat intelligence feeds to enhance detection rules?

- Do we monitor for indicators of compromise and suspicious behaviour?

Alerting and response

- Do we configure alerts for high-risk events?
- Do we ensure alerts are actionable and routed to appropriate teams?
- Do we integrate alerts into cyber security incident response workflows?

Event log analysis

- Do we conduct regular reviews of event logs for signs of compromise?
- Do we use automated tools to correlate events and detect patterns?
- Do we performed retrospective analysis after cyber security incidents?

Retention and compliance

- Do we retain event logs for a period consistent with legal and regulatory requirements?
- Do we ensure event logs are made available for forensic investigations and audits?
- Do we have documented event log retention policies?

How does your organisation manage legacy information technology?

Legacy IT presents significant and enduring risks to the cyber security posture of your organisation. The board should be aware that weak cyber security measures for legacy IT can increase the likelihood of a cyber security incident, and make any cyber security incident that does occur more impactful.

The most effective method to mitigate the cyber security risk posed by legacy IT is to replace it before it becomes unsupported. Retaining legacy IT within your organisation's IT environment, especially where adequate compensating measures 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 in your organisation.

ASD provides advice for executives to assist with legacy IT management.

Threshold governance questions

- Have we identified and documented all legacy IT in use?
- Have we assigned risk ownership responsibility for each piece of legacy IT?
- Have we established a legacy IT risk management strategy aligning with ASD's guidance?
- Have we assessed each piece of legacy IT for security vulnerabilities, operational dependencies and business criticality?
- Have we categorised each piece of legacy IT based on risk exposure and impact?

Supplementary technical questions

Compensating measures

- Do we have compensating measures for when patching legacy IT is not possible?
- Do we document, and regularly review, compensating measures for their effectiveness?

Access controls

- Do we restrict access to legacy IT to only those who need it?
- Do we log all access to legacy IT?

Monitoring and incident response

- Do we include legacy IT in our security monitoring and alerting activities?
- Do our cyber security incident response plans account for legacy IT?
- Do we conduct testing of cyber security incident response playbooks involving legacy IT?

Vendor support considerations

- Do we regularly scan for legacy IT that is no longer supported by vendors?
- Do we engage vendors for extended support or security advisories if available?
- Do we document end of life timelines and vendor support gaps?

Transition and decommissioning plans

- Do processes for secure data mitigation from legacy IT exist?
- Do we maintain a roadmap for replacing or retiring legacy IT?
- Do we prioritise decommissioning legacy IT based on risk and business impact?

How does your organisation manage its cyber supply chain risk?

The board should have oversight of how cyber security risk is managed in the cyber supply chain. Suppliers, manufacturers, distributors and retailers involved in products or services used by your organisation will present a cyber supply chain risk for your businesses. Likewise, you will present a cyber supply chain risk to your customers.

For Australian Prudential Regulation Authority regulated entities, there are specific obligations set out in prudential standards on the oversight of suppliers and the *Security of Critical Infrastructure Act 2018* has obligations that extend across various participants in the critical asset supply chain.

Effective cyber supply chain risk management ensures, as much as possible, the secure supply of products and services throughout their lifetime. This includes their design, manufacture, delivery, maintenance, decommissioning and disposal. Cyber supply chain risk management should form a significant component of your organisation's overall cyber security strategy.

ASD provides advice for executives to assist with cyber supply chain risk management.

Threshold governance questions

- Have we developed a cyber supply chain risk management policy?
- Have we assigned ownership for cyber supply chain risk across procurement, legal and cyber security teams?
- Have we identified all suppliers with access to our systems and data?
- Have we categorised suppliers by criticality and risk exposure?
- Have we assessed suppliers' cyber security posture using assessments or certifications?

Supplementary technical questions

Contractual measures

- Do we include cyber security requirements in contracts and service level agreements?
- Do we require suppliers to notify us of breaches, security vulnerabilities or changes in risk?
- Do we require compliance with ASD's *Information security manual* (ISM)?

Due diligence

- Do we conduct cyber supply chain risk assessments before onboarding suppliers?
- Do we verify supplier cyber security measures and cyber security incident response capabilities?
- Do we ensure suppliers understand and agree to our cyber security expectations?

Ongoing monitoring and review

- Do we monitor supplier performance and compliance with cyber security obligations?
- Do we review supplier risk profiles periodically?
- Do we track and respond to emerging cyber threats affecting our cyber supply chain?

Third-party access management

- Do we limit supplier access to only necessary systems and data?
- Do we implement cyber security measures, such as network segmentation and multi-factor authentication, for supplier access to our systems?
- Do we monitor and log supplier access to our systems?

Cyber security incident response and resilience

- Do we include cyber supply chain compromise scenarios in our cyber security incident response planning?
- Do we ensure suppliers have their own cyber security incident response plans and reporting mechanisms?
- Do we establish communication protocols with suppliers for coordinated responses to cyber supply chain compromises?

Does your organisation have a post-quantum cryptography transition plan?

The board should be aware that in the near future cryptographically relevant quantum computers will render most contemporary cryptography insecure. This will result in existing secure communications based on current cryptography technology becoming vulnerable to compromise.

As the creation of a cryptographically relevant quantum computer presents new cyber security risks, the board should oversee steps to anticipate future business requirements and dependencies for vulnerable systems during the transition period to post-quantum cryptography standards.

ASD provides advice for executives to assist with the post-quantum cryptography transition.

Threshold governance questions

- Have we acknowledged the long-term impact of quantum computing?
- Have we assessed the potential impact of quantum threats to our systems and data?
- Have we established a post-quantum cryptography transition plan?
- Have we assigned executive and senior management responsibilities for post-quantum cryptography transition planning and readiness?

Supplementary technical questions

Cryptographic inventory

- Do we document where cryptography is implemented within our organisation?
- Do we have an inventory of the cryptographic algorithms, protocols and libraries we use?
- Do we track and record our dependencies on vulnerable cryptographic algorithms?

Vendor and supply chain engagement

- Do we regularly engage with vendors to understand their post-quantum cryptography transition plans and readiness?
- Do we require vendors to disclose cryptographic dependencies and upgrade timelines?
- Do we include post-quantum cryptography considerations in our procurement and contract negotiations with vendors?

Transition planning

- Do we monitor ASD’s advice on planning for post-quantum cryptography?
- Do we have a roadmap for migration to quantum-resistant algorithms?

Testing and validation

- Do we first test quantum-resistant algorithms in non-production environments?
- Do we evaluate performance, interoperability and the security of quantum-resistant algorithms?

Policy and compliance

- Do we have updated cryptography policies that include post-quantum cryptography considerations?
- Do we comply with ASD's post-quantum cryptography standards?
- Do we track regulatory developments related to post-quantum cryptography?

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.

This publication includes content that was generated or assisted by artificial intelligence tools. All artificial intelligence-generated material has been reviewed by human contributors to ensure accuracy, appropriateness and alignment with ethical standards.

The Commonwealth and the AICD 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

Use of the Coat of Arms

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre

Australian Institute *of* Company Directors