Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Questions for boards to ask about cyber security

First published: October 2022
Last updated: October 2022

Introduction

Cybercriminals and state-sponsored actors are using sophisticated techniques to compromise Australian organisations. The ACSC responds to attacks against Australian organisations every day, with the biggest threats including:

- ransomware
- exploitation of security vulnerabilities
- software supply chain compromises
- business email compromise.

Simply installing the latest technology in your business is not sufficient. Failing to invest in your organisation's cyber security could lead to costly attacks, interruptions to operations, reputational damage, legal liabilities and more. Understanding and managing cyber security risks within your organisation – as with any other business risk – is a key responsibility to protect your organisation and shareholders.

Why should boards be concerned about cyber security?

If exploited by malicious actors, cyber security vulnerabilities have the potential to significantly disrupt your business operations, incur significant incident response costs, damage your organisation's brand and reputation, and depending on the response of the board, may be a cause of shareholder or regulatory action.
Managing this risk requires strong leadership from the board working in concert with executives and technical teams to understand an organisations exposure and take actions as appropriate to individual organisations. Encouraging an organisational design and culture that supports cybersecurity is important and supporting technical experts and IT departments is essential.

What is the organisation's threat and risk environment?

Understanding what IT Systems are critical to your core business and how could they be exposed is integral to managing cyber risks. In order to respond effectively, boards need to have an understanding of the risks facing by their organisations before they can respond effectively.

Do boards understand the organisation's threat and risk environment?

Boards should proactively build an understanding of their organisation's specific cyber threat and risk environment. Understanding and managing cyber security risk within the organisation, as with any other business risk, is a key responsibility to protect the company and its shareholders and an important aspect of fulfilling your duties and obligations as directors. The board should seek to understand as much as possible about cyber security risks with a view to understanding what information technology systems are critical for the organisation's core business, how they could be exposed to cyber threats and what mitigations are in place to control risks to those systems.

How can the board stay informed on the threat and risk environment?

It is crucial that directors, and executives, seek out the most accurate and timely information from reputable sources. Look within your organisation to your experts including the Chief Information Officer (CIO), Chief Information Security Officer (CISO) or IT Managers.

Consult reputable sources of information on the changing threat environment including the Australian Cyber Security Centre (ACSC), the UK National Cyber Security Centre (NCSC) and the US Cybersecurity and Infrastructure Security Agency (CISA).

Boards should ask CIOs or CISOs whether your organisation has joined the ACSC Partnership Program. Being a partner ensures that you have the most up to date ACSC information including sensitive reporting from the ACSC. Details are available through our ACSC Partnership Program.

Boards should also ensure that CIOs, CISOs or IT Managers are up to date with the latest patching and mitigation advice from key vendors and service providers.

As always, boards through their Audit and Risk Committees should conduct periodic audits of cyber security, and embed regular updates on cyber incidents, trends and risks as part of your audit and risk governance.

Does the organisation know what data is held and where it is stored?

Information is valuable. There are many adversaries who would benefit from having access to your organisation's information and data. Have you identified critical information of which the confidentiality, integrity and availability is essential to the function of your organisation? Consider not only the value of individual records but also the aggregated value of your information holdings. Understanding where this information and data is stored within your organisation is also critical in properly responding to an incident.

Do you know what hardware and software is used in your organisation?

Your organisation needs to identify what is vulnerable. Boards should be comfortable with the level of continual audit of ICT security and be able to identify impact and severity quickly when new vulnerabilities are discovered. This can include virtual servers hosted in the cloud.

Do we know if there are cyber risks in our supply chain?

Does your organisation depend on key business partners, for example, vendors that supply critical software that runs your business, or a third party with remote admin access to your organisation? Vulnerabilities in your supply chain could impact your organisation. Boards should engage with their CIOs and CISOs to make sure their supply chain risks are being managed.

How should boards mitigate cyber risks?

What cyber security framework are used in the organisation?

Boards should understand the strategies and tools their organisation is using to mitigate cyber threats. The ACSC Strategies to Mitigate Cyber Security Incidents is a prioritised list of mitigation strategies to assist organisations in protecting their systems against a range of cyber threats. The mitigation strategies can be customised based on your organisation's risk profile and the cyber threats that you are most concerned about.

While no set of mitigation strategies are guaranteed to protect against all cyber threats, organisations are recommended to implement eight essential mitigation strategies as a baseline. This baseline, known as the Essential Eight, makes it much harder for adversaries to compromise systems.

Does the organisation routinely update and patch its systems?

Many vendors react to vulnerabilities by releasing mitigations and patches for known vulnerabilities to their customers. Boards should be asking CIOs and CISOs whether the organisation have processes and tools to routinely identify vulnerable systems and patch systems and applications.

How mature is the organisation's cyber security?

Understanding your organisation's cyber maturity will help you to identify areas that require further investment. The ACSC's Essential Eight maturity model is valuable resource. It can be used to assess an organisations current maturity level and identify a pathway to a target maturity level.

How do employees or customers disclose vulnerabilities?

If your organisation has an internet presence or produces software for customers, organisations need to consider how customers, employees and security researchers are able to report any issues they find. Organisations should ensure that a technical point of contact is easily reachable to disclose vulnerabilities and enable a quick response.

As per the Australian Government Information Security Manual, you might also consider implementing or updating a vulnerability disclosure program. This will help your organisation engage with security researchers operating in good faith as they identify vulnerabilities in your systems.

What is the organisation's plan to prevent or detect cyber incidents?

Organisations should develop and enact plans to identify affected products and services. Boards should look to the CIO or CISO to adopt a methodical approach which identifies how the organisation's business is affected or at risk from cyber security incidents and provides clear actions to patch or mitigate the vulnerability to reduce exposure and risk. Large organisations will need a phased approach to manage this issue over many weeks or months, with teams able to sustain a response over the medium term.

Boards should engage with the CIO or CISO to determine what the organisation is doing to detect and prevent attacks, and if sound plans are in place to respond to an incident such as a ransomware compromise.

Cyber security is an ongoing process, not a product. To assist in defending your organisation against cyber threats, have you implemented appropriate cyber security governance, risk management, incident response and business continuity

frameworks? There is no silver bullet for cyber security, neither individual security products nor cyber insurance are complete solutions.

Does the organisation have an incident response plan?

Your organisation should have a cyber incident response plan to ensure an effective response and prompt recovery in the event security controls don't prevent an incident occurring. This plan should be tested and regularly reviewed.

To be effective, a cyber incident response plan should align with the organisation's incident, emergency, crisis and business continuity arrangements, as well as jurisdictional and national cyber and emergency arrangements. It should support personnel to fulfil their roles by outlining their responsibilities and all legal and regulatory obligations.

Does the board know its regulatory obligations?

In the event of a cyber incident, **boards may have regulatory obligations** such as those under the *Notifiable Data Breach Scheme* which requires all businesses covered by the *Australian Privacy Act 1988* to notify the Office of the Australian Information Commissioner and affected individuals when an eligible data breach has occurred. If you have identified a breach, it is important that your communication is transparent, honest and timely.

How should boards respond to a cyber incident?

Is the board prepared to respond to a cyber incident?

It is important your board has measures in place to respond to cyber security incidents when required. Consider discussing these questions as a board, with your executive team and with internal IT managers, or outsourced service providers to ensure you are equipped with the most relevant information.

There are significant time pressures for decision making when responding to a cyber security incident. As a board, you should ensure you are available and prepared to make critical decisions that might exceed the delegated authority of executives and update your organisation risk appetite statement as required by a dynamic situation.

Every organisation should have an incident response plan in place and regularly review and test it, to ensure an effective response and fast recovery following a cyber incident. Incident response plans should be tested with readiness activities that target strategic decision-making, operational and technical capabilities, strategic engagement and communications.

In the event of a cyber incident, it is important to have one person in charge of the incident response to ensure clarity and timely decisions on operational requirements, prioritisation, continuity and communications.

Boards should work with the senior executive team to ensure that roles, responsibilities, delegations and risk appetites in responding to cyber security incidents are clearly defined. Executives such as the CIO or CISO are ideally placed to lead the organisational response. Boards should also consider nominating a Director -- ideally with relevant cyber security, operations or risk management skills -- to interface between the Board and the senior executive team to ensure board level decisions can be made quickly.

Further information

The *Information Security Manual* is a cyber security framework that organisations can apply to protect their systems and data from cyber threats. The advice in the *Strategies to Mitigate Cyber Security Incidents*, along with its Essential Eight, complements this framework.

Further information on cyber supply chain considerations when selecting web conferencing solutions is available in the *Cyber Supply Chain Risk Management* publication.

Contact details

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