Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Questions for the board of directors to ask about cybersecurity

First published: October 2022
Last updated: December 2022

Introduction

The Australian Signals Directorate (ASD) responds to attacks against Australian organisations every day. Understanding and managing cybersecurity risks within your organisation, as with any other business risk, is a key responsibility in protecting your organisation and shareholders.

Why should we be worried about cybersecurity?

If realised, cybersecurity risks have the potential to significantly disrupt your business operations. This can result in significant cybersecurity incident response costs, damage to your organisation's brand and reputation, and depending on your response, shareholder or regulatory action.

Managing cybersecurity risks requires strong leadership with the board of directors working in concert with executives and technical teams to understand the organisation's risk exposure. Encouraging an organisational culture that supports cybersecurity is important, as is supporting technical experts and information technology (IT) departments in their cybersecurity efforts.

What is our threat environment?

Do we understand our threat environment?

Understanding what systems are critical to core business operations, and their security posture, is integral to managing cybersecurity risks. Furthermore, in order to determine cybersecurity risks, you need to have an understanding of the threat environment in which your business operates.

How can we stay informed of the threat environment?

It is crucial that you seek out the most accurate and timely information on cyberthreats from reputable sources, such as ASD. Also, look within your organisation to your experts, such as your chief information security officer (CISO), chief security officer (CSO) or chief information officer (CIO).

You should ask your CISO, CSO or CIO whether your organisation has joined ASD's Cybersecurity Partnership Program. Being a partner ensures that you have the most up-to-date cyberthreat reporting from ASD.

How can we protect our organisation and shareholders?

Do we know what data we hold and where it is stored?

Data is valuable. There are many malicious actors who would benefit from having access to your organisation's data. Have you identified critical data of which the confidentiality, integrity and availability is essential to the function of your organisation? Consider not only the value of individual pieces of data but also the aggregated value of your data holdings. Understanding where this data is stored within your organisation is critical to being able to both protect it and respond to a cybersecurity incident when it arises.

Do we know our regulatory obligations?

In the event of a cybersecurity incident, you may have regulatory obligations, such as those under the *Notifiable Data Breaches scheme*, which require you notify the Office of the Australian Information Commissioner and affected individuals when an eligible data breach has occurred. As such, in the event of an eligible data breach, it is important that you communicate this in a transparent, honest and timely manner.

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

Does your organisation depend on key business partners, such as vendors that supply software and hardware that supports your critical business operations, or a third party with remote access to your systems? Cybersecurity risks in your supply chain could impact your organisation. As such, you should engage with your CISO, CSO or CIO to make sure cyber supply chain risks are being identified and managed.

Do we know what cybersecurity framework we use?

Understanding strategies your organisation can use to mitigate cybersecurity risks is important. The *Strategies to mitigate cybersecurity incidents* is a prioritised list of mitigation strategies designed to assist organisations in protecting their systems and data against a range of cyberthreats. The mitigation strategies can be customised based on your organisation's security risk profile and the cyberthreats that you are most concerned about.

While no set of mitigation strategies are guaranteed to protect against all cyberthreats, organisations are recommended to implement eight essential mitigation strategies as a baseline. This baseline, known as the 'Essential Eight', makes it much harder for malicious actors to compromise your systems and data.

Do we know how mature our cybersecurity is?

Understanding your organisation's cybersecurity maturity will help you to identify areas that require further investment. The *Essential Eight maturity model* is a valuable resource in this regard as it can be used to identify priority areas for cybersecurity.

Do we know how security researchers and customers disclose vulnerabilities?

If your organisation has an internet presence or produces software for your customers, such as mobile apps, you should consider how security researchers and customers are able to report any vulnerabilities in your services or products that they find. This can be achieved through the establishment of a vulnerability disclosure program.

How should we respond to a cybersecurity incident?

Are we prepared to respond to a cybersecurity incident?

When responding to a cybersecurity incident, there are often significant time pressures placed on decision making. As such, you should be prepared to make critical decisions that exceed the delegated authority of your executives, such as your CISO, CSO or CIO. To prepare yourself, consider discussing the questions this publication raises with your executive team, and with any outsourced service providers, beforehand.

To further assist in preparing to respond to a cybersecurity incident, it is important that you have appropriate response measures in place, such as a cybersecurity incident response plan. To be effective, a cybersecurity incident response plan should align with your organisation's emergency, crisis and business continuity arrangements, as well as jurisdictional and national cyber and emergency arrangements. In doing so, it should support personnel to fulfil their roles by outlining their responsibilities and all legal and regulatory obligations. Such cybersecurity incident response plans should be regularly reviewed and tested alongside activities that target strategic decision making, operational responses and communication strategies.

Finally, in the event of a cybersecurity incident, it is important to have one person in charge as a cybersecurity incident response coordinator, such as a CISO or CSO, to ensure clarity of direction and timely operational decisions can be made. Ideally, this person should be supported by a board member with relevant cybersecurity or risk management skills in order to act as the interface between the cybersecurity incident response coordinator and the board of directors to ensure board-level decisions can be made and communicated quickly.

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.

Copyright

Use of the Coat of Arms

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

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

Australian Government
Australian Signals Directorate