Australian Government
Australian Signals Directorate

Questions for Boards to Ask About Cyber Security

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 cyber security 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 cyber security?

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

Managing cyber security risks requires strong leadership with the board working in concert with executives and technical teams to understand the organisation's risk exposure. Encouraging an organisational culture that supports cyber security is important, as is supporting technical experts and information technology (IT) departments in their cyber security 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 cyber security risks. Furthermore, in order to determine cyber security 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 cyber threats 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 Cyber Security Partnership Program. Being a partner ensures that you have the most up-to-date cyber threat 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 cyber security incident when it arises.

Do we know our regulatory obligations?

In the event of a cyber security incident, you may have regulatory obligations, such as those under the *Notifiable Data Breach 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 cyber security 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? Cyber security 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 cyber security framework we use?

Understanding strategies your organisation can use to mitigate cyber security risks is important. The *Strategies to Mitigate Cyber Security Incidents* is a prioritised list of mitigation strategies designed to assist organisations in protecting their systems and data against a range of cyber threats. The mitigation strategies can be customised based on your organisation's security 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 malicious actors to compromise your systems and data.

Do we know how mature our cyber security is?

Understanding your organisation's cyber security 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 cyber security.

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 cyber security incident?

Are we prepared to respond to a cyber security incident?

When responding to a cyber security 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 as a board, with your executive team and with any outsourced service providers beforehand.

To further assist in preparing to respond to a cyber security incident, it is important that you have appropriate response measures in place, such as a cyber security incident response plan. To be effective, a cyber security 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 cyber security 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 cyber security incident, it is important to have one person in charge as a cyber security 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 cyber security or risk management skills in order to act as the interface between the cyber security incident response coordinator and the board to ensure board-level decisions can be made and communicated 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.

Contact details

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