Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Planning for critical vulnerabilities: What the board of directors needs to know

First published: January 2022
Last updated: December 2023

Introduction

This publication provides information on why it is important that the board of directors is aware of and plans for critical vulnerabilities that have the potential to cause major cybersecurity incidents.

What are critical vulnerabilities?

Critical vulnerabilities are flaws in software, or in rarer cases hardware, that can be trivial to exploit and if left unaddressed can be used by malicious actors to gain control of systems, steal personal data or intellectual property, install malware or cryptocurrency mining tools, or perform ransomware attacks – with such events often significantly impacting business operations and reputation.

An example of a highly publicised critical vulnerability in late 2021 (known as Log4Shell) involved Log4j, a Java-based logging framework used in a wide variety of applications, such as messaging and productivity software, mobile device managers, teleconferencing software and web hosting software. At the time, wide-spread exploitation was occurring and over 100,000 products were impacted.

Why should the board of directors be concerned about critical vulnerabilities?

Critical vulnerabilities are a serious business continuity risk that have the potential to disrupt business operations, impose significant cybersecurity incident response costs, damage reputation, and depending on the response of the board of directors, may be a cause of shareholder or regulatory action. Often, the Australian Signals Directorate (ASD) will have observed the successful wide-spread exploitation of systems within Australia.

Notably, critical vulnerabilities are often easily exploited across the internet. Online services, such as web stores and other services used by customers, are most at risk of compromise and disruption. Other systems that supported business operations, such as teleconferencing or remote access solutions, may also be impacted and provide further opportunities for malicious actors to compromise organisations' internal networks and cloud environments.

Managing the risks associated with critical vulnerabilities requires strong leadership from the board of directors alongside efforts to work with senior executives and technical teams to understand their organisation's exposure. Encouraging an organisational culture that supports cybersecurity is important, and supporting technical experts within information technology (IT) departments is essential.

What questions should the board of directors be asking?

In the context of critical vulnerabilities, it is important that the board of directors has measures in place to respond to major cybersecurity incidents. As such, consider discussing the following questions with senior executives, and any outsourced service providers, to ensure your organisation is ready to respond to any major cybersecurity incidents caused by critical vulnerabilities.

What are the board of director's obligations?

Understanding and managing security risk within your organisation, as with any other business risk, is key to protecting the company and its shareholders, as well as an important aspect of fulfilling duties and obligations as Directors. In doing so, the board of directors should seek to understand as much as possible about security risks with a view to understanding what systems and data are critical for your organisation's core business, how they could be exposed to cyberthreats and what mitigations are in place to control risks.

If your organisation produces or distributes vulnerable software, it has a responsibility to identify whether this impacts your customers. For example, your organisation may have legal and contractual obligations to urgently develop patches for products and assist your customers to implement mitigations to reduce the likelihood of harm from critical vulnerabilities. Furthermore, the board of directors may have regulatory obligations such as those under the *Privacy Act 1988* and the *Notifiable Data Breaches scheme* which requires certain businesses to notify the Office of the Australian Information Commissioner and affected individuals when an eligible data breach occurs. If your organisation identifies a major cybersecurity incident, it is important that it is communicated in a transparent, honest and timely manner.

Finally, there are often significant time pressures for decision making when responding to a major cybersecurity incident. The board of directors should ensure they are available and prepared to make critical decisions that might exceed the delegated authority of senior executives or any outsourced service providers.

How is the board of directors and management team staying informed?

It is crucial that Directors, and senior executives, seek out the most accurate and timely information from reputable sources in order to stay informed. Look within your organisation to your experts, including the chief information security officer (CISO) and chief information officer (CIO). In addition, consult reputable sources of information on the changing cyberthreat environment and critical vulnerabilities. This should include vendors, ASD, the United Kingdom's National Cyber Security Centre (NCSC) and the United States' Cybersecurity & Infrastructure Security Agency (CISA). Finally, the board of directors should ask their CISO or CIO whether your organisation has joined ASD's Cybersecurity Partnership Program. Being a partner ensures that you have the most up to date reporting on critical vulnerabilities, including sensitive reporting.

As always, the board of directors, through your audit and risk committee, should conduct periodic audits of cybersecurity and embed regular updates on security risks and cybersecurity incidents as part of your audit and risk governance activities.

Who is leading on our response?

It is important to have one person in charge of the response to critical vulnerabilities, and any major cybersecurity incidents that arise as a result, to ensure clear and timely decisions on operational requirements, prioritisation,

continuity and communications. Senior executives such as the CISO or CIO are ideally placed to lead your organisation's response.

The board of directors should also work with senior executives to ensure that roles, responsibilities, delegations and risk appetites in responding to critical vulnerabilities are clearly defined. In addition, the board of directors should consider nominating a director – ideally with relevant cybersecurity, operations or risk management skills – to interface between the board of directors and senior executives to ensure board-level decisions can be made quickly.

What is our response plan?

Your organisation should develop and enact a plan to identify products and services affected by critical vulnerabilities. As part of this, the board of directors should look to their CISO or CIO to adopt a methodical approach that identifies how your organisation's business is affected or at risk.

As critical vulnerabilities often result in major cybersecurity incidents that have a long tail, and may require surge resourcing or the establishment of a dedicated tiger team to address, 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.

If your organisation is a vendor that produces or distributes software, the board of directors needs to know there is a clear plan to release patches or mitigation advice and how this will be communicated to customers.

Do we know what hardware and software we have in our organisation?

Your organisation needs to be able to identify what is potentially vulnerable as a result of critical vulnerabilities. As such, the board of directors should be comfortable with a level of continual audit for cybersecurity and be able to identify impact and severity quickly when new critical vulnerabilities are discovered. In the context of critical vulnerabilities, IT teams should be able to identify instances of affected software, and whether the vulnerable software is being used in the development of internal software. This task is often easier on corporately-managed assets, but unmanaged and Bring Your Own Device (BYOD) devices may also be at risk. The CISO or CIO should be thinking about how they will manage the risks associated with aging capabilities or capabilities that are not centrally managed or supported (often called 'legacy IT' and 'shadow IT' respectively).

Have we patched or mitigated the critical vulnerability?

Many vendors react to critical vulnerabilities by immediately releasing patches or mitigation advice for their customers. As such, the board of directors should be asking their CISO or CIO whether your organisation has patched all vulnerable systems and applications, and if a plan is in place to patch other systems and applications if more patches or mitigation advice becomes available at a later date.

How will we know if we are being attacked and can we respond?

The board of directors should engage with their CISO or CIO to determine what your organisation is doing to detect any attempts by malicious actors to exploit critical vulnerabilities, and if a plan is in place to respond to a major cybersecurity incident, such as a ransomware compromise or extortion attempt. Your organisation should also have a plan in place to continuously monitor your systems and data for signs of compromise.

How will people report issues they find to us?

With critical vulnerabilities, many security researchers will try to identify vulnerable software or hardware, which may include those your organisation depends upon or produces. To assist security researchers with such endeavours, you

should ensure that a technical point of contact within your organisation is easily reachable to facilitate a quick response to critical vulnerabilities which are identified.

In addition, if you do not already have one, consider setting up a help desk for your customers to call or email to seek advice on either how to mitigate critical vulnerabilities identified in your products or services or to understand how a major cybersecurity incident impacts them.

Finally, you might also consider implementing a vulnerability disclosure program, along with hosting a security.txt file on your website. This will help your organisation engage with security researchers operating in good faith as they identify critical vulnerabilities in your products or systems.

Do we know if our supply chain is affected?

If your organisation is dependent on key business partners, such as vendors that supply critical software that runs your business, or a third party with remote administrative access to your systems, you should have an open and honest conversation with them during any major cybersecurity incident, acknowledging that they may also be trying to understand the severity of any major cybersecurity incidents themselves. Work together with your vendors and suppliers to mitigate any critical vulnerabilities collaboratively.

When did we last check our business continuity and crisis management plans?

Finally, the board of directors should regularly verify your organisation's end-to-end business continuity and crisis management plans against cyberthreats to minimise real world impact to your organisation should a major cybersecurity incident occur.

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.

For more technical information about Log4Shell and the Log4j vulnerability, ASD released a *Mitigating Log4Shell and other Log4j-related vulnerabilities* advisory.

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.

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

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

Australian Government

Australian Signals Directorate