What Exactly is the Board's Role in a Cyber Incident?

Courtney Carr

ELGP 2026 Research Summary

Did you know that most cyber-attacks happen outside of business hours? [1] [2] Picture this, it's Saturday morning, you wake up, open your phone, and see that the organisation you are a Board Director for has become the victim of a cyber-attack. Would you know what to do? Would you be confident that your organisation is safe? If your answer is no, you would not be alone. A global survey of hundreds of directors and executives found that close to half of respondents felt either unsure or negative about whether their organisation's data was well-protected[3].

The reality is the role of the board in a cyber crisis begins well before the attack itself. Boards need to be confident that their organisation is prepared[4]. Cyber incident preparedness is a growing priority for board directors. The latest threat reports show an 11% increase in cyber incidents that the Australian Cyber Security Centre has responded to since prior year, and an 83% increase in the number of potential threats they have had to warn entities about[5]. This comes at a huge cost for organisations; medium size businesses saw a 50% increase in the average self-reported financial cost of cybercrime and large businesses 219%[5].

So how does the board prepare? We need to remember that it is not just large companies and governments that experience attacks. The Australian Charities and Not-for-profits Commission defines cyber security as the act of "*protecting your charity's electronic information from unauthorised access*" and advises all Responsible People of charities and not-for-profits (NFPs) to make sure they can identify and manage relevant cyber security risks[6].

Common risks for NFPs

- Attackers gain unauthorised access to systems (often via volunteer or staff accounts, especially when multi-factor authentication is not used)
- Viruses or other malicious software (malware) spread through the network
- Fake emails and websites used to trick staff into transferring funds or sensitive information (false invoices and requests to change bank details)
- Service disruption, costs, reputation damage[6].

Once cyber risks are identified, there are many controls that can be explored to manage those risks (board-level risk committees can assist with balancing the cost and effort against the benefits of risk mitigation). Examples of controls a board could consider[7]:

- Cyber security policy, risk framework and insurance
- Cyber included in risk appetite statements
- Scenario planning for cyber incident response (annual exercise at a board meeting or retreat)
- Promoting a culture of cyber resilience (to reduce the risk of human error)
- Information asset registers[8] (that identify sensitive and personal information)[9]

Now, back to our Saturday morning scenario, during the attack itself. A Board Director might need to become actively involved; your role will be to provide agile and timely support and oversight of management's key decisions[10]. If the attackers have locked you out of your systems (like what happened to staff from an Australian youth charity[11]) do you have a plan for how you would communicate with the rest of the board, executive team and key stakeholders?

What about after the incident? The board should oversee post-incident reviews and understand the impact of the attack (e.g. potential risk of harm to individuals and the cost of recovery). As well as oversee remediation efforts, such as dealing with claims or complaints that may arise, and supporting the review and update of cyber risks and related risk appetite statements[12].

While skilled operations teams may lead incident response to get your organisation back online, Directors should be prepared to support and are obligated to act with care and diligence[13]. Questions about cyber security are not something that can always be deferred to management to answer. Board members should be able to talk to the type of cyber threats their organisation faces and be aware of, and confident in, cyber incident response and recovery plans[14].

References

1. Lang, Michael, Lena Connolly, Paul Taylor, Phillip J. Corner, "The Evolving Menace of Ransomware: A Comparative Analysis of Pre-pandemic and Mid-pandemic Attacks:, *Digital Threats: Research and Practice,* Volume 4, Issue 4 (2023) https://dl.acm.org/doi/10.1145/3558006
2. Arctic Wolf, *2025 Security Operations Report*, AW_RP_2025 SECURITY OPERATIONS_NA_092522 (2025), 2025 Security Operations Report - Arctic Wolf
3. Deloitte, *Digital frontier: A technology deficit in the boardroom,* Digital transformation topics | Deloitte Insights
4. The Australian Institute of Company Directors, *Not-for-Profit Governance Principles,* Third Edition (2024), 46, aicd-nfp-governance-principles-2024
5. Australian Signals Directorate, *Annual Cyber Threat Report*, (2025), 18 & 47, ASD Cyber Threat Report 2024-25
6. Australian Charities and Not-for-profits Commission, *Governance Toolkit: Cyber Security,* Governance Toolkit: Cyber security | ACNC
7. The Australian Institute of Company Directors, *Not-for-Profit Governance Principles*, 44, 46 & 70
8. Australian Charities and Not-for-profits Commission, *Governance Toolkit*
9. Office of the Australian Information Commissioner, *Australian Privacy Principle guidelines: Chapter B: Key concepts*, Version 1.4 (2022), Chapter B: Key concepts | OAIC
10. The Australian Institute of Company Directors, *Governing Through a Cyber Crisis*, (2024), 6, governing-through-a-cyber-crisis-280324
11. Australian Charities and Not-for-profits Commission, *Governance Toolkit*
12. The Australian Institute of Company Directors, *Governing Through a Cyber Crisis*, 8
13. The Australian Institute of Company Directors, *Cyber Security Governance Principles,* Version 2 (2024), 14, cyber-security-governance-principles-web3
14. Deloitte, *Digital frontier: A technology deficit in the boardroom*