Guardians of digital trust
Cybersecurity Awareness Month

How boards can enhance their cybersecurity knowledge

Six strategies to protect your organisation from cyber threats

BDO

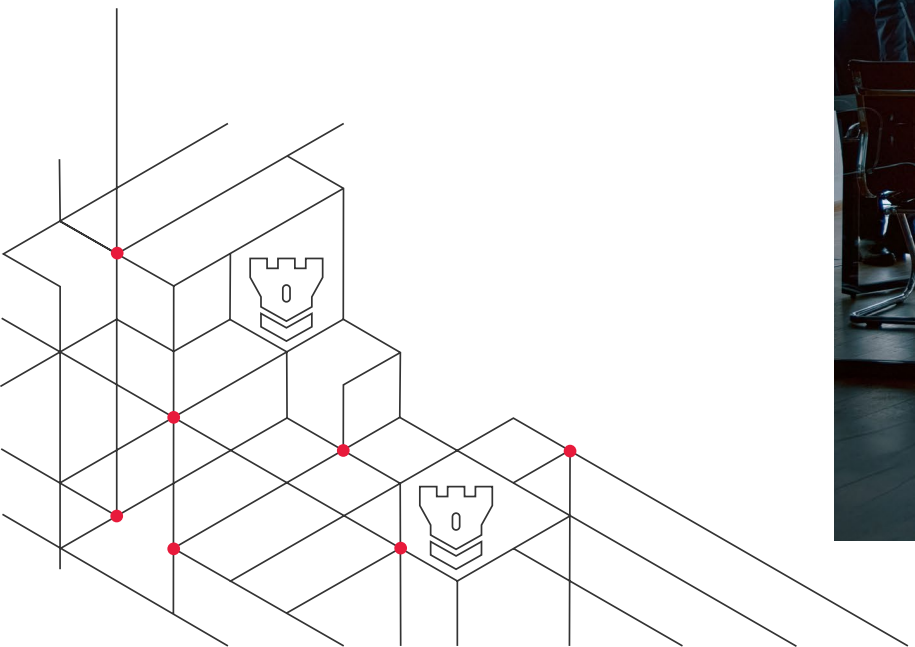
How boards can enhance their cybersecurity knowledge:
Six strategies to protect your organisation from cyber threats

Cybersecurity incidents are not only increasing in frequency, but also in cost.

In fact, the global average cost of a data breach in 2024 is $4.88 million, which is a 10% increase from 2023. It's also the highest cost to date. Of course, financial repercussions are not the only cost organisations face when they deal with a cybersecurity incident — as reputational and operational damages can also cripple the business.

Board members must play an active role in mitigating and preventing cyber-attacks. However, only 12% of S&P 500 companies have a current or former board member that is a cyber expert. This knowledge gap may be hurting your organisation now and in the future.

How can you ensure your organisation doesn't end up in the latest cybersecurity breach news cycle? It starts with asking the right questions.



Navigating today's cybersecurity landscape: Areas of focus for the board

Technology capabilities have grown significantly over the years, empowering organisations to operate more efficiently and drive expedited outcomes. As technology becomes increasingly intertwined with business objectives, board members need to evaluate technology decisions in the same way they evaluate strategic business decisions. Just as the board guides an organisation's business direction, it is also now responsible for ensuring that the correct technology elements are enabled to support the business strategy and the right level of cyber risk tolerance is achieved and managed.

To ensure responsible oversight, the board should focus on the following areas:

01

Strategic alignment

Ensure that cybersecurity initiatives are aligned with the business and technological goals of the organisation. To be proactive, boards should also as ensure future risks and trends are considered.

02

Regulatory compliance

Provide oversight of the organisation's compliance with relevant regulations and laws. This includes ensuring that the required audits and assessments are performed and that the board has insight and a clear understanding of the results.

03

Governance and oversight

Oversee the organisation's cybersecurity-related policies, strategies, and alignment with the overall risk management framework. The board should understand relevant cyber risks to the organisation and ensure that established policies support mitigation.

04

Monitoring and reporting

As a board member, it's important to make sure you receive regular updates regarding the cyber health of the organisation, including progress on key cybersecurity initiatives, key metrics, and key performance indicators.

05

Expert engagement

Engage with cybersecurity experts, either through the appointment of a cyber expert to the board, leveraging a CISO on the management team, or consulting an external Virtual CISO (vCISO). This will ensure the board is well informed on emerging threats and trends.

06

Cyber incident response

Ensure the organisation has a defined incident response programme and they regularly review updates on the results of incident response testing. In the event of a cyber incident, the board should play a role in overseeing how the organisation communicates with the public and stakeholders.

Six strategies to increase your cybersecurity knowledge

For boards to successfully oversee their organisation's cybersecurity programme, bridging the current knowledge gap is essential. This will help ensure cybersecurity is adequately addressed in regular board meetings and allow boards to confidently carry out their duties where cybersecurity is concerned.

Here are six strategies you can use to build your knowledge and become more prepared to integrate technology risk into decision-making processes:

01

Establish regular cyber education sessions.

Ensure you are getting regular updates about cybersecurity. During these sessions, carve out time to discuss the top risks in your industry and relevant experiences of similar organisations, and ask questions around what your business is doing to mitigate, prevent, or respond to the risk of those types of incidents happening to your organisation. The answers you receive may be key in strengthening your organisation's defence framework.

02

Refocus the metrics and leverage industry benchmarks.

It's important to shift the focus from technical metrics to common sense metrics that highlight risk and value. For example, identifying the number of end-of-life systems with vulnerabilities and the controls in place to mitigate their risks, or discussing the complete costs of cyber breaches, which includes the actual response team, legal support, as well as the impacts to insurance premiums and the organisation's revenue. Use industry benchmarks to compare your organisation with others in your vertical, helping you understand where the organisation stands and what improvements are required.

03

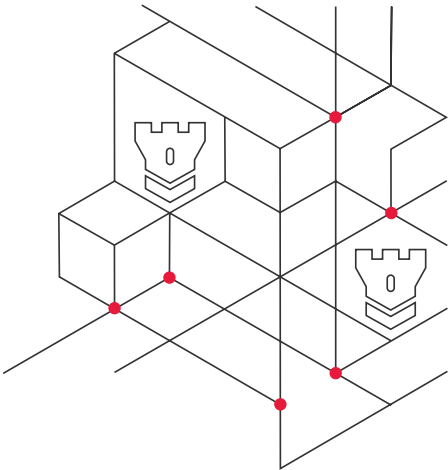
Bring in external cybersecurity experts.

By bringing in external cybersecurity experts, board members can not only enhance their cybersecurity knowledge, but also get support "translating" technology-focused information into risk-focused insights and strategies. Ultimately, adding a cyber seat to the board will offer regular access to the expertise you need that complements your organisation's risk management, security, and technology teams.

04

Conduct cyber simulations.

To get a deeper understanding of actual cyber threats and how to respond to them, consider hosting facilitated incident simulations. These exercises will help you understand your role as a board member during a cyber event, potential impacts, areas for continuous improvement in process flows, and build muscle memory.



05

Provide oversight during an incident.

In the event of a cyber-attack, board members should actively engage with and receive updates from the security experts and incident response teams. By staying updated on the incident progress and outcomes, they can offer independent oversight and ask questions to uncover any lingering risks. It's also important for boards to understand how the organisation plans to respond to future cyber-attacks.

06

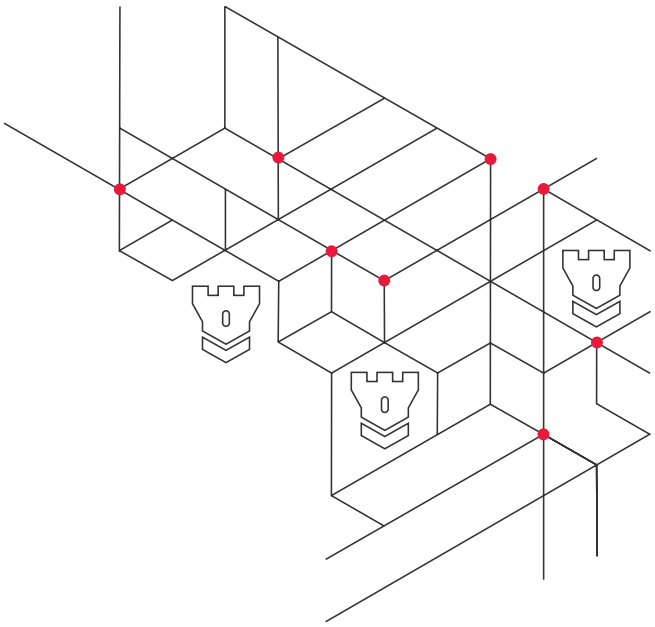
Look back with hindsight.

What you can learn from close calls or even a previous cyber incident may be what stops it from happening again, especially since 83% of organisations have had more than one cybersecurity breach. Ask how many times these close calls or actual incidents have happened and what the organisation has learned to identify gaps and develop appropriate measures.

The board's critical role in managing cyber risk

What has changed in recent years is the level of scrutiny around the board of directors. After all, boards are there to help the organisation manage risk—and that includes risks from cybersecurity incidents.

In a recent Gartner study, 88% of boards of directors said they view cybersecurity as a business risk, which highlights the move to prioritise cybersecurity as a focus of the board. It is your fiduciary duty to not only provide independent oversight to manage the company's cybersecurity posture, but also to challenge your organisation in different ways to raise the bar for your defence framework.

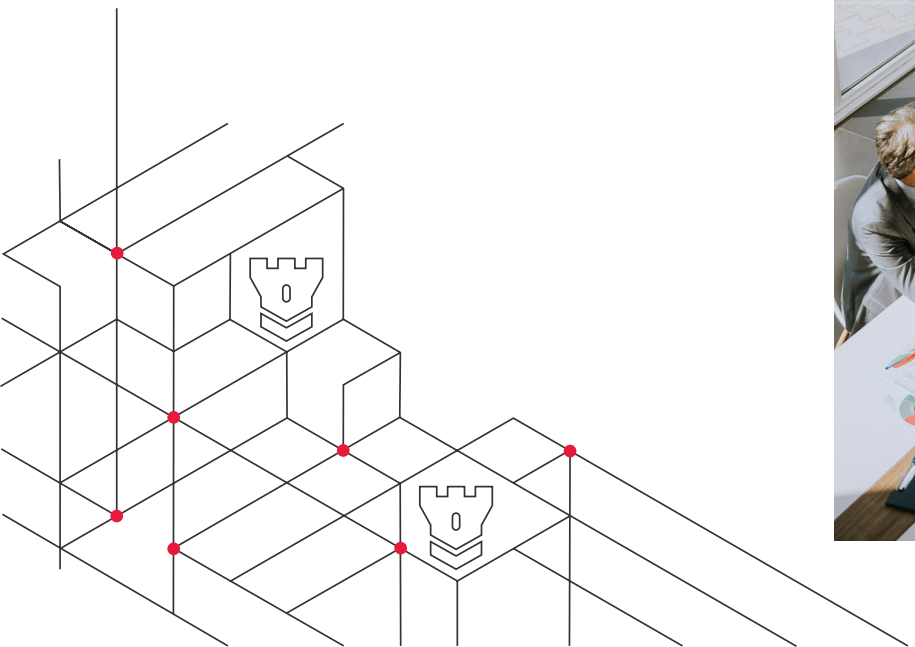


How BDO can help

At BDO, our approach to cybersecurity includes a business focused approach for managing cyber risk. We offer board education sessions to help bridge the knowledge gap and enable board members to stay ahead of the rapidly evolving technology landscape. In these sessions, we show board members how to refocus a technology-centred conversation into one about business risk, so that boards can effectively offer a responsible level of oversight and ask the right questions of their teams. Our board education sessions also cover the latest cyber risks organisations are facing today and what organisations are doing to mitigate those threats.

CONNECT WITH OUR CYBERSECURITY LEADERSHIP TEAM TODAY

Enhance your knowledge of cybersecurity and be prepared for whatever the threat landscape brings next.



'BDO', 'we', 'us', and 'our' refer to one or more of BDO International Limited, its network of independent member firms ('the BDO network'), and their related entities.

The BDO network is an international network of independent public accounting, tax and advisory firms which are members of BDO International Limited and perform professional services under the name and style of BDO (hereafter: 'BDO member firms'). BDO International Limited is a UK company limited by guarantee. It is the governing entity of the BDO network.

Service provision within the BDO network is coordinated by Brussels Worldwide Services BV, a limited liability company incorporated in Belgium.

Each of BDO International Limited, Brussels Worldwide Services BV and the BDO member firms is a separate legal entity and has no liability for another entity's acts or omissions. Nothing in the arrangements or rules of the BDO network shall constitute or imply an agency relationship or a partnership between BDO International Limited, Brussels Worldwide Services BV and/or the

BDO member firms. Neither BDO International Limited nor any other central entities of the BDO network provide services to clients.

BDO is the brand name for the BDO network and for each of the BDO member firms.

© Brussels Worldwide Services BV October 2024