SETTING THE TONE FROM THE TOP:
THE ROLE OF THE BOARD IN *CYBER* SECURITY

BDO

The rapid growth in innovation and technological developments has delivered substantial productivity improvements across all markets, both in Australia and globally. However, the rise of e-commerce and widespread internet connectivity also expose individuals, businesses and IT systems to cyber risks which cyber criminals are exploiting.

Cyber risk landscape

Businesses face a range of cyber risks, both external threats and internal vulnerabilities that continue to evolve over time. In recent years, there has been significant growth in the number and severity of cyber attacks around the world. The estimated annual cost of cyber attacks to the global economy is more than $400 billion. Recent studies suggested that in 2013, cyber attacks affected 5 million Australians at an estimated cost of $1.06 billion. As well as these direct costs, cyber attacks may:

- Result in significant opportunity costs for an organisation - for example, through stolen intellectual property, or
- Undermine confidence in an organisation and damage its reputation in the community—for example, through data and privacy breaches as a result of cyber attacks.

It is not possible to protect against all cyber security risks. As cyber attacks continue to increase in complexity and sophistication, more organisations will experience cyber attacks. It is therefore important that organisations seek to improve their overall cyber resilience in order respond to and recover from an attack as quickly as possible.

With this in mind, the need for Boards to have a thorough understanding of their risks, and how to mitigate against, and recover from cyber attacks, is now fundamental to business survival. It is imperative that Boards treat cyber security with the same level of importance as they would manage 'traditional' risk, such as OH&S (Occupational Health and Safety) and reputational risks.

On the surface, achieving this focus at the Board level may seem challenging, but it can be done in a way that delivers significant benefit to the organisation. By taking a structured and analysis driven approach, the Board can take the organisation on a journey to achieving cyber security resilience, ensuring they have full awareness of the organisation's cyber risks, threats, plans and continual improvement measures.

This eBook provides guidance on the steps you can take to get your Board on the path to engaging a cyber-savvy mindset. We cover off on how to assess your cyber threats, how to identify your organisation's critical digital assets, and how to develop a tailored cyber security strategy which will make your organisation more cyber resilient.

LEON FOUCHE
Partner, Risk Advisory
Tel: +61 7 3237 5688
leon.fouche@bdo.com.au
https://www.linkedin.com/in/leonfouche

Take off the blinkers…cyber risk isn't about IT

Despite the growing number of high-profile data breaches, many Boards often don't have an in-depth knowledge of cyber risks. Many Board members don't have a background in IT security, which means they are often lacking the basic technical knowledge to fully understand these risks and their potential impacts on the business.

The growing complexity of these risks, in terms of both their sources and style, means Boards must focus on becoming more cyber-aware and embedding this way of thinking into the organisation at every level.

A whole of business issue

One of the biggest challenges with cyber risk is that many decision makers still view it as an issue for the IT department. Cyber risks impact the whole business which requires a risk management approach to be driven from the very top. This involves integrating cyber risk management into the Board's current risk management strategy in exactly the same way as it would manage the more 'traditional' risk, such as OH&S and reputational risk.

Responsibility of the board

The Federal Government is moving to introduce mandatory breach disclosure legislation requiring organisations to report suspected cyber breaches to the Privacy Commissioner. The potential for Boards to be held legally responsible for a lack of oversight, coupled with increasing regulatory pressures, means that cyber risk warrants a comprehensive strategy led by the Board.

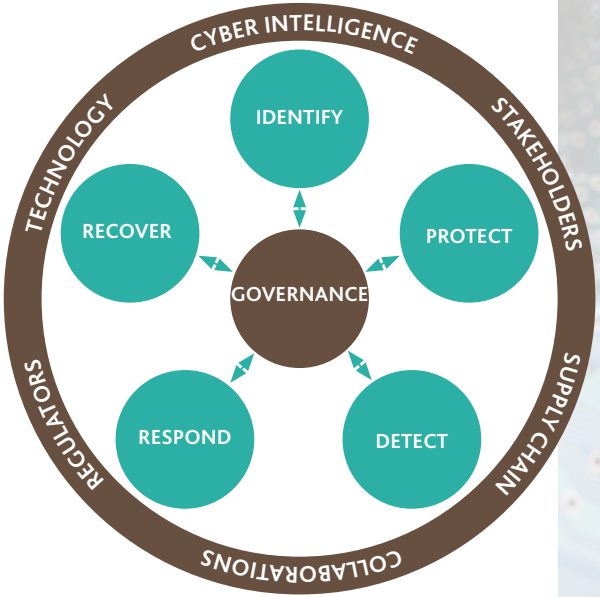
Building your organisation's cyber resilience

Cyber resilience is the ability to prepare for, respond to and recover from a cyber attack. Resilience is more than just preventing or responding to an attack - it also takes into account the ability to operate during, and to adapt and recover, from such an event.

The goal for any organisation must be to become more cyber-resilient. This involves integrating a range of cyber risk assessment activities into the Board's realms of responsibility. Doing this properly is best achieved by executing, and continually reinforcing, a proven Cyber Resilience Framework. This allows an organisation to take a strategic view of its entire cyber security risk management lifecycle and ensure it aligns with its business plans.

The BDO Cyber Resilience Framework is based on industry best practice and goes well beyond a traditional, compliance driven information security model. The core components of our framework assist organisations to:

- *Identify* their most critical intellectual property and digital assets
- Develop and implement procedures to *protect* them
- Put in place technology, procedures and resources to *detect* a cyber security incident
- Put in place procedures to both *respond* to and *recover* from a cyber incident, if and when one occurs
- Define effective *governance* to manage cyber risks across the entire organisation.



Let's take a closer look at how to apply this framework.

Identify and understand your potential sources of cyber risk

The first step is to assess the current cyber risk landscape and how these threats will impact the organisation. When reviewing the potential threats, there are a number of external and internal threat actors or adversaries to consider. Both these groups warrant the attention of the Board in order to understand how threats from each category might affect the organisation.

The main external threats include:

- **Cybercriminals:** Those adversaries seeking to profit from acquiring an organisation's information
- **Hacktivists:** Individuals or groups with a political or ideological motivation for targeting an organisation's digital assets
- **State-sponsored groups:** Those adversaries performing cyber attacks for state-guided political or economic reasons, for example adversaries seeking to get access to intellectual property or adversaries seeking to damage or disrupt the systems (cyber terrorists).

Internal threats include:

- Employees who might inadvertently expose or share sensitive documents or open malware infected emails or documents that affect the organisation's data and IT systems
- Disgruntled employees deliberately targeting their employer systems and data to disrupt or cause reputational damage.

Know what needs protection

When it comes to cyber risk, not all systems and information are business critical to your organisation from a business interruption perspective. Boards looking to build better resilience against cyber risks must obtain a good understanding of what the business' critical digital assets are, that is, the systems and information so central to the business that you can't afford for them to be lost or disrupted through a cyber attack.

From there, it's important to assess the security measures in place to protect these digital assets and what the impact will be if these are compromised.

BDO USA's 2015 Board Survey found that only one-third (34 per cent) of respondents have completed documentation and assessments of their business critical digital assets and developed solutions to protect them.

It's important this assessment is done on a regular basis, as it identifies changes in the risk landscape and highlights the organisation's current cyber risk posture. If this exceeds your risk appetite, then further resources should be allocated to cyber security efforts to reduce the cyber risk posture for these assets.

Be prepared to respond

As the number and sophistication of cyber attacks increase, so will the likelihood increase that your organisation will be exposed to a cyber incident. It is important that organisations have a Cyber Incident Response Plan in place so they can detect, respond to, and recover from, these incidents. BDO USA's 2015 Board Survey found that less than half of respondents (45 per cent) have a cyber breach/incident response plan in place.

It is important that this Cyber Incident Response Plan is regularly tested and validated, as doing so will ensure business leaders are prepared and able to provide support to the organisation during a cyber attack. The Board needs to be included in this process as this will improve the directors' general awareness of cyber risks and what their role is in responding and recovering from a cyber attack.

Cyber resilience must be driven from the top

The Board has an important role to play in setting the tone for the organisation as a whole. Ultimately, everyone in the organisation has a role to play in upholding the security of the organisation, but the Board must lead the way so every level of the business is aware of the cyber risks they face and how to effectively respond and recover from a cyber incident.

As with every aspect of risk management, responsibility for cyber risk stops with the Board. Those Boards that are proactive on this front and focus on building that cyber-resilience will be far better placed to navigate these new risks and emerging cyber threat landscape.

As we've discussed, building a cyber-resilient organisation is no longer a job for IT alone. It requires the Board to invest time in understanding the threat landscape, identifying the digital assets they can't afford to lose and then developing an appropriate cyber incident response plan which is regularly reviewed. This way, the Board will not only meet their compliance requirements, they can also build a cyber-resilient organisation.

Tailoring an approach to your needs

At BDO, we understand that cyber security risks are evolving and that it is imperative that businesses keep pace with managing these risks. We work with our clients to assist them with developing a tailored cyber resilience strategy.

Our cyber security services include:

- **Strategy and governance** – what is your current level of cyber resilience and how can it be improved?
- **Risk and compliance** – are you adequately addressing your cyber risks and compliance requirements?
- **Assessment and testing** – how susceptible are your systems to cyber attacks?
- **Incident response and investigations** – do you have effective cyber incident response plans in place and have you incorporated lessons learnt from prior cyber incidents?
- **Awareness and education** – do you have effective security awareness and education programs in place?

Contact us if you want to know more about how to enhance the cyber resilience of your organisation by creating a cyber-savvy Board.

BOOK YOUR FREE CONSULTATION HERE

NEW SOUTH WALES
NORTHERN TERRITORY
QUEENSLAND
SOUTH AUSTRALIA
TASMANIA
VICTORIA
WESTERN AUSTRALIA

1300 138 991
www.bdo.com.au

Distinctively different – it's how we see you

AUDIT • TAX • ADVISORY