Unveiling the Invisible Threat:

Mastering the Art of Conveying Cyber Risks to Boards

itnews

CHECK POINT™

Boards play a key role in securing budget and executive sponsorship for cybersecurity programs, while non-executive directors can also be held personally liable if their business suffers a cyberattack.

It is therefore crucial for chief information security officers (CISOs) to learn to better communicate cyber risk to boards, to ensure that the appropriate level of risk awareness and investment is directed towards cybersecurity.

In this iTnews roundtable sponsored by Check Point Software Technologies, and in partnership with AusCERT, a group of CISOs from Australian end-user organisations discussed their stakeholder management strategies, challenges and successes, to better leverage the board to drive cyber resiliency in their organisations.

> **"even if expertise exists in house to address concerns raised by boards, having a trusted outside source present clear, agreed messaging to the board can bolster funding**
>
> **MIKE HOLM,**
> SENIOR MANAGER AT AUSCERT

Boards understand risk

While some attendees suggested that boards are more knowledgeable about cybersecurity than they are given credit for, and have in the last 12 months, become much more informed on the topic, others highlighted the need for board members to take responsibility for their own learning when it comes to cyber awareness.

The table unanimously agreed, that ultimately, what boards understand is risk.

One attendee suggested that boards' understanding of cyber risk is a similar journey to that of OH&S. In that sense, it's about board directors understanding the critical functions that need to be protected, and how cyber strategy or risk mitigation is improving the business' ability to protect these functions.

According to Mike Holm, senior manager at AusCERT, while some CISOs would argue that board directors are not interested in granular detail, his experience has proven otherwise.

"Although traditional thinking is that boards aren't interested in details, during recent briefings we've given we've been asked questions like "how did the ransomware attack on QUT happen and what controls could we implement to avoid similar attacks here?". Therefore, when communicating to boards, certainly focus on mitigating risk, but be prepared to dive into details if asked," Holm said.

"In some cases, even if expertise exists in house to address concerns raised by boards, having a trusted outside source present clear, agreed messaging to the board can bolster funding for and solidify acceptance of a cyber security management program."

When asked to describe the key methods that CISOs have found to be most effective in communicating cyber risk to boards, responses included:

- **Avoid technical jargon**
- **Display information using dashboards and graphs**
- **Create a narrative story that is easy to explain**
- **Give real world examples**
- **Touch on up-to-date topics that board members are aware of, such as news regarding changing legislation or recent hacks**
- **Find allies from other areas in the business, such as OH&S, and present together**
- **Learn the 'language' of the board, and adopt their language when presenting**

According to attendee Alexander Moskvin, CISO at Steadfast Group, the method he has found most effective is to focus on the data, and numbers that are related to the organisation.

"Select two to three messages and focus on them," he said.

Ashwin Ram, cyber security evangelist at Check Point Software Technologies, believes that CISOs should keep the discussion relevant by using case study examples specific to the sector within which they work.

Ram also suggested, "Identify a champion in the board who can act as your mentor – this person can be your sounding board and help you navigate board communication."

The Australian Institute of Company Directors (AICD) and the Cyber Security Cooperative Research Centre (CSCRC) partnered to publish a set of Cyber Security Governance Principles designed to provide a

clear framework for directors to build stronger cyber resilience.

One attendee pointed to this tool as a starting point for directors when it comes to cyber security governance.

The principles are as follows:

1. **Set clear roles and responsibilities**
2. **Develop, implement and evolve a comprehensive cyber strategy**
3. **Embed cyber security in existing risk management practices**
4. **Promote a culture of cyber resilience**
5. **Plan for a significant cyber security incident**

Quantifying cyber risk

For CISOs to achieve non-executive director buy-in for cyber investment, cyber risk needs to be directly correlated to the value, and impact to the business.

One way of quantifying cyber risk is to outline the business impact of what a loss of a particular system for a day, a week or longer would mean for the business.

Taking an approach that looks at identifying the critical impact areas, matching controls and articulating to the board the cost of these controls in line with the impact of these systems being shut down, presents a better risk-based approach for board directors.

According to AusCERT's Holm, it's important to draw out a realistic risk appetite statement from the board.

"Considering the type of business involved, there could be human lives at stake. At the very least, there will always be financial loss to consider. Then, how to actually quantify risk will depend on each organisation and their established risk appetite.

"For example, a small online retail business may have determined that more than two days of system outages would result in insolvency, therefore a prolonged denial of service attack could qualify as an extreme or unacceptable risk," he said.

Executives may use cyber risk quantification as a means of communicating risk in terms of dollar value.

Check Point's Ram suggests four key steps for cyber risk quantification:

1. **"Understand your assets. The more you know about your environment, the better your risk quantification will be.**
2. **Identify your threats. You need up-to-date threat intelligence to identify what might be at risk.**
3. **Carry out risk assessments. This will help you understand where you are vulnerable and work out the likelihood and impact of each risk.**
4. **Deploy counter measures. This could involve fixing software vulnerabilities or making configuration changes."**

"Quantifying cyber risk is an ongoing process, not a set and forget. Your risk will change over time, so you need to regularly review your assessments and make changes as needed. The key to cyber risk quantification is automation. Gaining near real-time understanding of your posture is vital," said Ram.

"Regardless of the cyber risk quantification (CRQ) model used, it is essential to consider the business context, IT context, and cyber security context to obtain a comprehensive view of the breach risk to an organisation."

Questions from the board

It's a board director's job to ask questions – and sometimes the kinds of questions that they are asking can be reflective of their level of knowledge when it comes to cyber risk.

But how should CISO's handle difficult questions or pushback from the board?

According to AusCERT's Holm, anticipating the kind of questions that board directors may ask, will come down to having an understanding of the board's point of view.

Holm said, "In this current climate, a board might well ask "what would we do if a ransomware attack resulted in double extortion with subsequent data leakage?" The answer may well be "we have mitigatory controls to prevent data exfiltration in the first place" but that's not what the board asked – they're assuming the worst and expecting you to say something like "if our data is found on the dark web, we have an existing (paid) arrangement with ID Care to provide recovery assistance to customers".

> **"Dealing with pushback means you didn't understand all your key stakeholders and what their motives are**
>
> **ASHWIN RAM,**
> CYBER SECURITY EVANGELIST AT CHECK POINT SOFTWARE TECHNOLOGIES

Check Point's Ram believes it comes down to preparation.

"Firstly, it is important to be well prepared for meetings. This means circulating board briefing papers well in advance and seeking feedback prior to meetings with the board. Dealing with pushback means you didn't understand all your key stakeholders and what their motives are," he said.

When roundtable attendees were asked which question that they wished board directors would ask more often, answers included:

- **How can we help drive cyber resilience strategy?**
- **What do you need to prioritise in your cyber strategy, to ensure our organisation is suitably geared towards preventing attacks?**
- **Are all key stakeholders participating in breach simulation exercises (tabletop)?**
- **Can you present the findings from our last breach simulation exercise?**
- **Do you think our expectations regarding cyber risk management are realistic and if not, why not?**
- **How can we learn more about our role in managing this risk?**

Creating a cyber-resilient culture

While digital tools are important in preparing organisations against cybercrime, human behaviour and cyber resilient cultures can be just as important and sometimes harder to maintain.

According to Holm, board directors play a key role in propagating a culture of cyber resiliency.

"Whilst the role of a board member does not include operational duties, it absolutely is the board's role to set a risk appetite and most importantly, a culture within the organisation. It's important to set a culture of honest incident and risk reporting, no blame or recriminations for honest mistakes, and a learning culture," he said.

"This is important to ensure that employees feel comfortable reporting incidents and risks, allowing management to adequately deal with them and conduct post incident reviews openly with the view of improving the organisation and its individuals for the next cyberattack."

While cybersecurity may have historically relied only on technology, the strongest mitigation strategies incorporate controls at both the people and process layers, Holm explained.

"A successful cyber security risk management program needs to address all those elements, and with significant expertise in each. Often that expertise can't be found in one individual, so this means a successful cyber security team requires very diverse skills."

SUPPORTED BY

CHECK POINT™

itnews