SideBoard

Conversations that matter for non executive directors

The essential guide to managing cyber security

Cyber crime is now the number one threat to business growth, according to Australia's CEOs. With attacks jumping 109% over the last 12 months, cyber has become the most common economic crime in Australia [global economic crime survey 2016].
Yet boards are struggling to keep up. Two leading cyber experts, Telstra's Mike Burgess and PwC's Richard Bergman, answered NEDs' questions about how to get on top of the escalating risk.

Q. What is the key principle to managing cyber?

One of the most common mistakes we see is companies trying to manage cyber as a technology issue. But it's not – it's a business risk and it should be managed just like any other business risk, such as economic risk or strategic risk. For the last 10 years most companies have been throwing money at technical solutions and they simple haven't worked; the attacks and the costs are still increasing. That's because cyber is essentially about people and criminal intent – the technology is just the means to an end. So companies that are already good at managing risk will also be good at managing cyber, if they view it in the same way.

Q. What are the most important things to know; what should Boards be asking?

A big part of the challenge for boards is getting the right sort of information from management. Too often they're presented with highly technical reports that simply don't address the critical questions. People are often the weakest link when it comes to cyber security, so it's important that the problem is framed in a way that shifts the focus off technology and onto risk.

Telstra has come up with the 'Five Knows of Cyber Security' that companies need to know to make the right decisions about managing cyber. If you're unclear on the 'Five Knows of Cyber Security' for your organisation, then you should be concerned:

1. **Know the value of your data.** You need to know what value it has, not just for your organisation and customers, but also the value to those who may wish to steal it. All data has value to someone.
2. **Know who has access to your data.** You need to know who has access both within an organisation and externally, like who has 'super user' admin rights in your organisation and within your trusted partners and vendors.
3. **Know where your data is.** You need to know where the company's data is stored. Is it with a service provider? Have they provided data to other third parties? Is it onshore, offshore or in the cloud?
4. **Know who is protecting your data.** You need to know who is protecting your valuable data. What operational security processes are in place? Where are they? Can you contact them if you need to?
5. **Know how well your data is protected.** You need to know what security professionals are doing to protect the company's data 24/7. Are employees, business partners and third party vendors who have access to data adequately protecting it?

Cyber crime is now the number one threat to business growth with attacks jumping 109% over the last 12 months.

Cyber is a business risk and should be managed as other organisational risks e.g. economic and strategic risk.

The Five Knows of Cyber Security

- *Know the value of your data.*
- *Know who has access to your data.*
- *Know where your data is.*
- *Know who is protecting your data.*
- *Know how well your data is protected.*

pwc

Q. How secure can you really make the company?

Put simply, you can't ever be 100% secure. All companies must assume that if they haven't been breached yet, then they will be at some point in the future. The key is to stop focusing on building a 'hard perimeter'. Instead, invest more in capabilities that increase the speed of detection and the effectiveness of your response. Research shows that cyber intruders are inside an organisation for 240 days, on average, before they are detected. That's a lot of time to be looking for data to steal or systems to disrupt. If companies can get better at detecting threats, they can minimise the scale of impact.

Q. What makes an effective response to a cyber attack?

An effective response is one that limits the damage and cost to the business while protecting – or even enhancing – the company's reputation and trust with its customers. Loss of trust can be one of the biggest and most enduring impacts of a cyber attack. Unfortunately most companies are still not adequately prepared for, or even understand the risks they face from cyber. A recent global survey conducted by PwC found that only 37% of organisations have a cyber incident response plan in place *[global economic crime survey 2016].*

Q. What about securing my personal data?

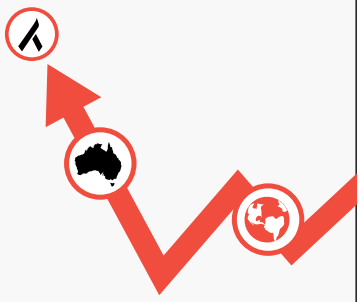
Unfortunately, cyber crime is often personal. And because NEDs are high profile individuals, they are particularly susceptible. We see this a lot during M&As and corporate transactions, where hackers attack the personal or home accounts of board members associated with a deal. The competitive landscape is such that now nation states are often the source of deal related cyber attacks, as a means of getting inside knowledge or information that may provide a commercial advantage. NEDs should ask themselves the same five questions about cyber security that they ask company management.

Cybercrime awareness in Australia is growing at a rate far greater than the rest of the world

The perception of the risk of cybercrime is on the rise – ***80%*** for Australia versus ***53%*** globally and ***68%*** for the US.

Almost two thirds of Australian respondents told us they'd been affected by cybercrime.

Most reported crime in Australia in this year's survey, though only ***42%*** of respondents have a fully operational incident response plan.



PwC's Global Economic Crime Survey 2016

Understand cyber by trying it yourself

Guests of PwC's NEDs program got to experience first hand what a cyber attack feels like by playing Game of Threats™, a digital game designed to simulate the speed and complexity of an actual cyber breach. The game provided an interactive experience where one team tried to defend itself from a team of threat actors (from the same company). It creates a realistic, fast environment that rewards good decisions, and penalizes bad one. Players walked away with a much better understanding of the steps required to better secure their companies.
Find out more at *http://www.pwc.com.au/cyber/game-of-threats.html*

Cyber intruders are patient, they can be inside an organisation for 240 days on average.

Cyber on the Board agenda;

- *Understand the Five Knows of Cyber Security*
- *Boards need the right information from management.*
- *They need information that addresses the critical questions above.*
- *Start thinking of cyber as any other business risk.*
- *Ask management "What is the company's cyber incident response plan?"*
- *NEDs should ask themselves the same critical questions as organisations, when it comes to securing their personal data.*

For more information on issues relevant to Boards in Australia please contact our Chairman

Michael Happell michael.j.happell@au.pwc.com *https://au.linkedin.com/in/mjhappell*

For more information on Cybersecurity please contact:

Steve Ingram steve.ingram@pwc.com *https://au.linkedin.com/in/steve-ingram-89395224* or

Richard Bergman richard.bergman@pwc.com *https://au.linkedin.com/in/richard-bergman-a987b973*