GE's top global cybersecurity manager has checklist for NZ directors

April 2016

Speed read

At the Institute of Directors' annual conference last week in Auckland, Tim MacKnight, the global chief information security officer (CISO) at GE, had a checklist for how directors should manage cybersecurity.

With cyber risk at GE among the biggest in the world, across all countries and multiple industries from finance, to consumer products, to infrastructure, his views and experience have some force. CISOs are increasingly being appointed by companies to manage cybersecurity issues, given it is a multi-disciplinary area, beyond the ICT team and into HR, communications, finance and legal.

What Mr MacKnight suggests overlaps with what we think is a legal obligation on directors. Most boards breach their cybersecurity legal obligations, which are to apply the IOD's Cyber Risk Practice Guide (or similar).

This article was first published in National Business Review.

The Detail

We have earlier explained why most boards likely do not comply with their legal requirements.

Tips

Tim MacKnight summarised his hints for directors with this list:

- Educate yourself on cybersecurity
- Add cyber security to your agenda – it is not just an "IT" issue
- Understand legal issues
- Define roles and responsibilities – who is responsible for what
- Know your crown jewels
- Assess your security posture (framework)
- Leverage your industry and share approaches and intelligence with others

He also emphasised the need to do what he called tabletop exercises to practise and plan what happens when there is a cyber breach, bringing together the stakeholders such as ICT, cybersecurity, HR, comms, legal, board, chief executive and so on to run through various potential scenarios. We've also concluded that boards have legal duties too, to ensure their companies have

adequately planned for what to do when there is a cyber breach.

Reputational risks

Businesses suffering a cybersecurity breach of its customers' financial and other confidential data will surely suffer damage to their hard-earned trust and favourable reputation, Pead PR managing director Deborah Pead says.

> *"These businesses can also be held liable for the restitution to all parties affected by a successful attack and that can result in severe financial losses incurred by the business. It is no longer a matter of 'if' but 'when'. And when it happens, among other things, businesses need to have a cybersecurity issues management plan ready to implement alongside the information security, communications and legal teams to protect their reputation and restore trust,"* Ms Pead says.

Where does cybersecurity risk fit?

Mr MacKnight said that, for GE, cybersecurity is now the No 4 risk issue for the GE board and management. And that applies throughout the world, in countries large and small, and in companies, large and small. (GE still has an interest in small suppliers to its businesses having strong cybersecurity and does strong due diligence and monitoring).

Although each company has its own issues and risk rankings, the recent New Zealand IOD-Marsh survey of directors has a similar outcome: the directors ranked cyber security as the second highest organisational risk for their organisations. The highest is reputational risk, and cyber breaches, in turn, have major reputational considerations. Now maybe putting cybersecurity at No 2 has it ranked too high when thinking about the many issues for boards. But what is clear is that cybersecurity is right up there.

Wigley+Company
PO Box 10842
Level6/23 Waring Taylor Street, Wellington
T +64(4) 472 3023 E info@wigleylaw.com
and in Auckland
T +64(9) 307 5957
www.wigleylaw.com