Cybersecurity for the IRO

It's not "if" you'll experience a cyber incident; it's "when" – according to an article run in NIRI's IR update from May 2016.

Cybersecurity involves protecting sensitive electronic data, whether it's in customer records or company records and documents. The value of sensitive information is a powerful attraction for hackers – but employee negligence is also a significant factor in cyber incidents. And the cost to a company of a cybersecurity breach is high – both in terms of direct costs, but even more critical is the potential damage to a company's reputation and revenue as those impacts can have lasting or even devastating effect.

A US study from 2015 reveals that 60 per cent of small businesses go out of business six months after a publicly disclosed data breach. IROs typically work for larger organisations, but they also face real and serious cybersecurity threats.

Companies are increasingly focusing on mitigating cybersecurity risks, but they face many challenges: limited budgets, competing priorities, and ever-changing and advancing technology. Time is also a big issue; a cyber incident can occur in a few minutes, but not be detected for months, and how to find the perpetrators?

A growing corporate governance issue

In the US cybersecurity incidents rose by 55 per cent from 2014 to 2015, and that trend is only rising. Given this, and the financial and operational implications, cybersecurity is becoming an increasingly important corporate governance issue. Consequently, the majority of public company board members as well as corporate management indicate that this is an increasing risk management concern.

Not surprisingly, cybersecurity is an issue of increasing concern to investors as well. Institutional investors are now looking more closely at what companies – and their directors are doing to oversee and mitigate risk. This is why it is also increasingly important to the IRO on multiple levels – e.g. protection of sensitive data, ensuring that a company crisis plan is in place and making sure to be part of the crisis team when communicating to the market what your company is doing should an incident occur.

Preparation is key

Having a robust cybersecurity program is critical to managing and mitigating the legal and business risks, and having a robust plan and an incident response plan firmly in place before an incident can reduce the costs of a data breach both financially and when it comes to loss of company reputation.

Remember: you never know who the hackers might be or what their intentions are by inflicting a security breach. Just because they can, could be the perfect reason for hacking.