CYBER SECURITY & RISK

THE NEW AND EMERGING CRIME ON COMPANIES

Prepared for Directors & Senior Management of Clients of AEI Group

Parts of the following document were authored by Mr Andrew Penn, CEO Telstra

MAY 2017

Cyber-security and cyber risk are no longer on the periphery and are (or should be) occupying the minds of every company director & senior manager as attacks increase in number and sophistication and the potential damage, when internal processes are not properly followed, can be catastrophic.

A problem for Senior Management though can be penetrating the tech-speak so common in the cyber world so they can look squarely at the risk, ask the right questions and ensure they are making the right decisions.

With so much at stake, Andrew Penn, CEO of Telstra, shared a framework that may help company directors think about what is a critical issue. Here is what he said.

"An (un)clear but very present danger

Not long ago I was enjoying a conversation with a senior policy maker when he asked me how many attempted cyber-attacks we had on our networks in the course of an average month. He hazarded a guess: might it be two or three attacks a month? No I told him, we had probably had two or three attacks since you started asking the question!

I share that story to make two points. Firstly, cybercrime, hacktivism and online espionage are happening every day, every hour, every minute, and every second (our recently released Cyber Security Report found that most Australian businesses have their security breached every month). The second point is that even among very senior leaders – government, community and business – there is often not a good level of understanding around the scale, tempo or sophistication of cyber risk and cyber-crime.

Why is cyber risk such an issue?

Cyber risk is a big issue and it is getting bigger all the time because accelerating technology innovation means the number of digital applications and services we use, either as individuals or organisations, is increasing rapidly. Moreover these applications and services are now (almost without exception) connected to a network. That means the barriers to entry for those that would do us harm – whether they are criminals, terrorists, activists, nation states or otherwise – have come down dramatically. A digital world means it is now possible to potentially rob a bank from the other side of the world and undertake all manner of illegal activities without detection.

The challenge with cyber risk is its intangibility. In a physical world it is easy to form a firm opinion about levels of security because you can see it with your own eyes. We know Fort Knox is more secure than a suburban bank branch because we can see the relative levels of security in the form of armed guards, security cameras, surveillance equipment, safes, and strongrooms and so on.

It is much harder to do that in a cyber world when the threat is invisible and often intangible. Put another way, you would not think of walking down a dark alley at 2 am in a dodgy neighbourhood in a city you have never been to before but how do you know that, metaphorically speaking, you are not already doing just that when you go online?

Too tactical or too technical

The challenge for Directors (and particularly Directors who do not have a good grounding in technology) is that too often discussions and briefings on cyber security are overwhelmingly technical.

Cyber experts and oracles by necessity come from deeply technical backgrounds and their views and advice can get very technical and very tactical very quickly. Complex briefings on issues like denial of service attacks, hacking, phishing and malware are not always easy for Directors to understand much less form an informed opinion about the relative impacts, implications and appropriate responses.

To be effective, Directors need a real sense for what the whole landscape looks like so they can anchor their thinking about an issue. They need to be able to interrogate the strategic thinking and decision making and be certain in their own minds that the risk is being managed appropriately. But if you cannot translate the tech-talk into plain-speak it is very difficult to know if you have done everything you can to mitigate cyber risk within your organisation and whether you have appropriate rectification strategies in place when issues arise, because one thing which is almost guaranteed is they will arise.

How to anchor Boardroom thinking around cyber risk

Notwithstanding these challenges (and the fact that the methods and technique of cybercriminals constantly change), cyber risk in reality is just like any other risk a Board considers. Behind the complexity, cyber-crime is just crime, cyber espionage is just espionage and hacktivism is just activism all by another name.

The key is to be able to cut through the technical language and get an understanding of the whole cyber landscape. We think there are three elements to the cyber risk equation:

1. Understand your context. *Whether you are (a transport & logistics company, manufacturer, retailer or professional service provider), context is important because it determines where you need to focus your risk management activities. One important aspect of this is your data, which is ultimately the asset which is at risk from a cyber-attack. At Telstra we have developed what we call the Five Knows of Cyber Security, a series of key questions to focus our thinking. We have found this useful in bringing a down to earth approach to a complex issue and that has helped improve understanding from the Board down. The Five Knows are 1) knowing the value of our data, 2) knowing who has access to our data, 3) knowing where our data is, 4) knowing who is protecting our data and 5) knowing how well it is protected. When you can answer these five questions you are in a better position to effectively assess and manage cyber security risk.*

2. Manage cyber risk like any other risk. *At Telstra we use the traditional three lines of defence risk model. The first line of defence are the processes, technologies and people within the core business that have accountability for protecting against risk. Ultimately accountability for risk management has to be embedded with the relevant line management. The second line of defence is typically the policies and standards that define risk appetite and approaches. The Chief Information Security Officer (CISO) plays a key role here. The third line of defence is typically some form of audit conducted from time to time to ensure the controls that are in place are working. This means a new set of skills for the internal audit function to develop. Like any risk it is also important to think about cyber risk through the process in which it occurs. The better you understand the environment which creates the risk, the better positioned you will be to predict, prevent, detect, respond and remediate it should it occur and data analytics can also play an important role in each stage of the process. This includes the discipline of a post-event remediation and rectification process to ensure we learn everything we can from the experience and use that knowledge to continually improve our processes, our people and our technology, to stay ahead of the risk.*

3. Managing cyber risk is not just about technology. *It is also about people and process. You can have the best technology in the world but if your people inadvertently give away their passwords or do not follow processes, you are likely to be exposed to cyber risk. Too often cyber security and cyber-risk management strategies focus on deep technology solutions and not enough on people and process.*

An example I often use to highlight this point is the common cybercriminal ploy of dropping malware infected USB sticks at the location of a target and waiting for an employee to pick one up and plug it into a desktop somewhere on the network.

A Board challenge

The days when cyber security and cyber risk were an 'IT issue' are long gone. ***Today they have the potential to ruin businesses, wreck reputations and compromise customer data and as such belong in the Boardroom****. The challenge for Directors is peeling back the layers of complexity and being able to manage it like any other risk.*

The ability to do that will define the future success of the companies they lead."

AEI's View

Apart from reliance on good preventative risk management measures implemented by your IT Manager, Contractor or indeed yourself, Cyber Attacks are constantly evolving and keeping up with new and innovative methods of attack can be overwhelming and or indeed impossible.

Transferring some this crime exposure to an insurance policy specifically crafted to protect you in three important areas is in our opinion now a mandatory insurance policy in the same manner that you insure your Assets against Damage and your business against Public Liability claims.

We have seen clients who have been significantly affected by the installation of Ransomware by hackers which happened to infect their backups and rendered their current and backed up data unable to be used. The costs to replace POS machines, servers, software etc has been significant. Thankfully they were insured.

There are three main components of a Cyber Liability & Privacy Protection Insurance cover:

1. Third Party Claims - covers the your potential liability to third parties from a failure to keep data secure, such as claims for compensation by third parties, investigations, defence costs and fines and penalties from breaching the Privacy Act

2. First Party Costs - reimburses your costs incurred to respond to a breach, such as IT Forensic Costs, Credit Monitoring Costs, Public Relations Expenses and Cyber Extortion Costs (including ransom payments to hackers)

3. Business Interruption - this section provides reimbursement for your loss of profits resulting from the breach, as well as any additional necessary expenses it may need to incur to continue business as usual

The insurance industry and AEI Group are ready to take on the challenge of assisting businesses in providing protection against this evolving modern day risk.

We encourage you to speak with us today if you are concerned about these exposures and wish to transfer these risks to an affordable insurance policy.

Finally some statistics worth sharing……