Rethinking Cyber Risk:
board and director obligations in 2015 and beyond

Dudley Kneller

A quick guide for directors and officers to addressing cyber security risks in governance processes
The World Economic Forum’s Global Risks 2015 report included a worldwide warning to all companies: 90% of companies worldwide recognize they are insufficiently prepared to protect themselves against [cyber attacks].¹

What many directors and company secretaries fail to realise is that the foundation of effective cyber risk awareness is just a matter of good corporate governance. With mandatory data breach reporting now almost inevitable in Australia and already in place in the United States and some parts of Europe, it is no longer appropriate to push responsibility for cyber compliance on to an IT department or technology provider.

Boards can no longer delegate their duties without understanding and actively managing the real risks associated with cybersecurity.

While we are yet to see an Australian cyber breach that takes directors to court, changes to the Privacy Act 1988 as well as an increasing “cyber awareness” from regulators such as the Australian Securities & Investments Commission (ASIC) and Australian Prudential Regulation Authority (APRA) firmly place cyber risk issues on the agenda for directors and officers.

Cybersecurity breaches are clearly on the rise

The KMART and David Jones cyber breach events that occurred in early October 2015² are a fresh reminder of the increasing risks that cyber breach events now pose to all Australian companies, as well as their directors and officers.

It remains to be seen whether Australian companies are likely to face the same challenges faced by Target in the US, which saw at least two shareholder actions filed against its officers and directors following a breach event.³


² See for example, Moncrief M “Kmart online customers’ information hacked in security breach” Sydney Morning Herald 1 October 2015 and Ockenden W, “David Jones computer system hacked and customers’ private details stolen” ABC News 2 October 2015.

³ See for example, Clark M “Timeline of Target’s data breach and aftermath: how cybertheft snowballed for the giant retailer” International Business Times 5 May 2014.
How do cybersecurity breaches occur?

There are three main ways that cybersecurity breaches can occur. They are:

- as a result of a criminal and/or malicious attacks (i.e. hacking);
- through the negligence or mistakes on the part of employees or contractors; or
- as a result of technology or system failure.\(^4\)

Sometimes the breach can be inadvertent, often occurring by interception of email or other data communications. Equally common is the risk of loss of sensitive information or data caused by insiders such as employees who have security clearance to access network and communications systems.

---

Corporations Act

Corporates should be aware that company directors need to be adequately informed of the risks of security breaches involving a breach of directors’ duties or other liability under the Corporations Act 2001 (Corporations Act).

Directors should consider the risk of shareholder litigation against the board if a breach does occur and it comes to light that the board failed to take reasonable steps to mitigate the risks of cybersecurity breaches. In limited circumstances, directors may be exposed to liability for criminal prosecution.

A breach of a director’s duty of continuous disclosure or duty of care and diligence under the Corporations Act may expose that director to a claim from shareholders, and a range of other affected stakeholders. The breach of duty of care and diligence was examined in the Centro Case in relation to the failure to disclose errors in the company’s financial statements. In this case, the proper approval of financial statements by the board was clearly viewed as an important element of good corporate governance. Although to date it remains untested, it is increasingly likely that effective data security and cyber risk management will be regarded in a similar light in future.

ASIC

A recent report issued by ASIC, Report 429 ‘Cyber resilience: Health check’ outlines a number of considerations as follows:

a. licensees are expected to address cyber risk as a key issue under their Australian Financial Services Licence (AFSL) and any applicable APRA compliance obligations;

b. cyber risks may need to be properly disclosed in a product disclosure statement or prospectus;

c. cyber risks may need to be disclosed in periodic reports such as an annual directors report - particularly for listed companies;

d. a cyber-attack may trigger a listed entity’s continuous disclosure obligations; and

e. directors must take into account cyber risks when discharging their duty to act with due care and diligence.

G Golding “Tightening the screws on directors: care, delegation and reliance” (2012) 35(1) UNSWLJ 266.
APRA (Financial services and AFSL holder specific regulations)

Additional obligations exist for organisations which hold an AFSL, some of which are regulated by APRA. APRA requires businesses to have clear accountability and communication strategies in place to limit the impact of data breaches, in addition to disclosure obligations if a major security breach does occur.

Privacy Act

Any company with a turnover of more than AUD $3 million (as well as some smaller organisations and government agencies) are subject to the Privacy Act 1988 (Privacy Act). Boards will need to take into account the risks of a failure to secure data where that failure results in a breach of the Privacy Act.

The Privacy Act requires entities to take reasonable steps to protect personal information such as customer details. Significant penalties may apply if you are responsible for a breach of the Privacy Act, including fines of up to AUD $340,000 for individuals and AUD $1.7 million for corporations, as well as the potential for compensation orders to be awarded.

Specific privacy obligations under Australian Privacy Principle 11

Australian Privacy Principle (APP) 11 requires that

An APP entity... must take reasonable steps to protect personal information it holds

(a) from misuse, interference and loss; and

(b) from unauthorised access, modification and disclosure.

In 2014, the Office of the Australian Information Commissioner (OAIC) was concerned that that Optus had not taken the necessary “reasonable steps” to comply with APP 11 following three significant privacy incidents, where the security of personal information held by Optus was compromised. The OAIC accepted an enforceable undertaking submitted by Optus that it would complete an independent review of its security systems and would implement any recommendations following the review.

Whilst the alleged breaches did not lead to any pecuniary penalty, the management time, legal and technology costs as well as ongoing compliance costs of the undertaking are significant and likely to exceed any financial penalty option available to the OAIC.

---

6 Office of the Australian Information Commissioner “Australian Privacy Commissioner accepts enforceable undertaking to enhance information security at Optus” media release (27 March 2015). See www.oaic.gov.au

7 Singtel Optus Pty Ltd Enforceable Undertaking Under s 33E of the Privacy Act 1988 (Cth) (2015) p 4
Contractual Obligations

Whilst Australian law relating to personal actions for breach of privacy is still in development, Australian companies need to consider the risks of litigation resulting from a breach of contract relating to data security, privacy or breach of confidentiality. In the event of a breach, contractual agreements in place may result in companies being liable for damages claims for a breach of their contractual obligations.

For example, commercial technology contracts are increasingly dealing with cyber security obligations as major risk elements with higher liability thresholds.

Litigation

Shareholder and customer actions are becoming more frequent as consumers become more aware of their own rights and plaintiff law firms push the class action agenda with the support and backing of large litigation funders now present in Australia. Large scale class action litigation in the United States is commonplace and is now occurring in relation to data security breaches. Notable cases include litigation following the Target breach and the Sony Playstation breach.

Directors are at risk under the Australian Consumer Law if they are found to have “aided or abetted” or “been in any way, directly or indirectly, knowingly” involved in the misleading and deceptive conduct of their company. Whilst this is a high standard to prove we expect it to be tested as the risks associated with cybersecurity breaches slowly make their way on to board meeting agendas.

---

*Sidel R “Target to settle claims over data breach”. The Wall Street Journal 18 August 2015.

*See post by Patrick Seybold, Sony Computer Entertainment America then Senior Director, Corporate Communications and Social Media, “Update on Playstation Network and Qriocity”, 20 April 2011, accessed 20 October 2015, http://blog.us.playstation.com
The Ponemon Institute published its global analysis study of the cost of data breaches in 2014, revealing that in 2014, the average cost to a company of a data breach increased by 15 per cent on the previous year. Given that the costs of data and cyber breaches is only expected to increase, it is important that boards understand the total costs of a breach and how they are incurred.

Financial impacts
In 2013, the average cost of a data breach in Australia was estimated at AUD $141 per record for each compromised record and a total organisational cost of AUD $2.7 million. The costs associated with responding to an event and remedying the breach are generally easy to identify, however some 'hidden costs' can be difficult to quantify. For example, it is often difficult to put a dollar value on the financial impact of reputational damage if it is not immediately reflected in revenues.

Loss of data
From an organisation perspective, the most obvious risk is the loss of commercially sensitive information such as the loss of trade secrets or disclosure of personal information. The remedies available for breach of confidentiality include taking action to try and compensate for the loss and damage suffered by such breach. However, damages are not always an adequate remedy.

It is well known that once confidentiality is lost, it cannot be regained. It is important that boards of companies can demonstrate they are taking necessary preventative measures to properly protect and secure information.

Reputation & goodwill
Damage to reputation is a critical risk to consider. A high profile security breach can result in damage to a business’ brand and goodwill as well as a loss of trust in the firm. Immediate losses associated with reduced trade may be measurable but there is significant risk of continued and future loss of trade and reductions in revenue associated with reputational damage following a cybersecurity breach.

This is a particular risk that may be difficult to assess and quantify if the reputational damage is sustained.

Many businesses who have been impacted by cybersecurity breach events struggle to manage this external “comms” piece. Boards need to ensure this aspect of the company’s response to a breach is carefully managed. Often communication to the market, media and other interested parties comes too late following the event or is inaccurate.

---


What do the regulators say?

Office of the Australian Information Commissioner (OAIC)

In 2014, the OAIC published guidelines relating to data breach notification12 and in January 2015 it published new guidelines on ‘taking reasonable steps’ to securing personal information13.

Together these guidelines provide useful insight into the regulator’s approach to the responsibility of businesses for information security generally and compliance with the Privacy Act.

Essentially, the OAIC is encouraging a top-down approach and recommending that businesses see information security as a corporate governance matter that requires an integrated approach. On this view, management, with board oversight, should be involved in establishing guidelines and providing sufficient oversight within the organisation to set the tone for a culture that is both security aware and accountable.

Australian Investments and Security Commission (ASIC)

In March 2015, the ASIC released a report titled Cyber resilience: Health check14. It indicated that ASIC intends to play a greater role in improving the cyber resilience of regulated entities and intends to incorporate cyber resilience into its surveillance activities.

The report identified regulated ‘licensee’ entities as having particular legal and compliance obligations that may require them to review and update their cyber risk management practices.

It also endorsed the US National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework)15 as a useful resource for regulated entities and indicated that it is particularly relevant to licensees.

---

Mitigating the risks – what can board directors do?

In an environment of rapid technological advancement and reliance on networked communications and IT systems, it is inevitable that breaches will occur and the sources of cybersecurity threats will continue to be ever changing.

While directors and boards should not be responsible for day-to-day implementation of technology strategy - this may be the role of a steering committee or Chief Information Officer - ultimately they are obligated to take an active role from a governance perspective.

This includes:

- taking reasonable steps to protect and maintain information and the security of the company’s network;
- protecting the company in the event of a breach; and
- ensuring all public statements relating to the breach and the company are accurate (to avoid false and misleading comments).
How?

- **Build a culture of compliance and cybersecurity awareness** starting from the top down. Appropriate governance frameworks, policies and procedures need to be in place for all information management activities, as well as adhered to and understood across the entire organisation. An education initiative may need to be undertaken first, particularly if there is a lack of understanding at board level. Ignorance is unlikely to be a successful defence should a director liability suit arise.

- **Ensure adequate budget allocation** to ensure reasonable steps can be undertaken. The company may need to invest in assistance with reviewing cybersecurity risk and response capabilities periodically to ensure that systems are keeping up with technology and developments in the regulatory environment.

- **Engage external counsel** if in-house capabilities are not skilled in this area of law and the network of legislation that governs it.

- **Have a network to draw on** should a breach occur. There is no point sourcing vendors and advisors once a breach has occurred. Ensure the board has a planned response team consisting of both internal and external advisors that can readily execute the incident response plan.

- **Appoint a leader** to be responsible for managing security, response team if required and regularly provide recommendations and reporting to the board. It is important for boards to have the involvement and input of someone with skills in cybersecurity systems and a thorough understanding of digital threats, opportunities and obligations - in particular legal compliance obligations. Some companies have a dedicated Chief Information Security Officer in charge of the information security program.

- **Consider cyber insurance** and whether it is appropriate for your business. Cyber insurance policies provide specific cover for liability and expenses incurred by a business as a result of a data breach or cyber attack. These events are often excluded from standard business policies, particularly where they relate to privacy or breach of confidentiality. As noted by a leading global cyber insurance provider, “insurers are denying coverage rather than willingly paying for a large catastrophic loss [unless they have specific cyber insurance].” A review of your cybersecurity risk profile will assist the board to assess whether a separate cyber insurance policy is warranted.

---

Conclusion

To determine whether a director has discharged their duty satisfactorily, the Courts will balance the reasonably foreseeable risk of harm against potential benefits that could reasonably have been expected to accrue to the company from the conduct.

Given the stance regulators and government are taking on cyber risk, boards which ignore cyber risk do so at their own peril.

Recent cases in the United States and now increasingly Australia indicate that both regulators and the Courts are at tipping point and will look to come down hard on those companies who fail to adequately address cyber risk.

About the Author

Dudley Kneller, Partner
Madgwick

Dudley Kneller is a technology lawyer and specialises in advising on strategic sourcing and supply projects, and procurement projects generally. He has more than 18 years’ experience practicing across Australia, Europe and the UK, and has worked on projects based in a range of countries, including the Philippines, India, and Russia and throughout South America. His clients span a broad range of industries, including technology, financial services, superannuation, retail and manufacturing.

Madgwick is a Melbourne-based law firm. We advise local, national and international clients on a broad range of matters including corporate and commercial law, property law, personal and corporate insolvency and dispute resolution. Our lawyers understand the changing nature of the regulatory and commercial environment in which boards and directors operate, and regularly advise on complex shareholder issues, directors’ duties and other corporate governance matters including cyber risk.
About LexisNexis®

LexisNexis provides world-class content and leading-edge technology to those who advance commerce, society and justice. Every day, more than five million legal, risk management, corporate, government, law enforcement, tax, accounting and academic professionals in over 100 countries on six continents rely on us to inform their decisions.