DLA PIPER

CYBER RISKS AND THE IMPACT ON COMPANY DIRECTORS

May 2014

A series of high profile data breach incidents have brought into spotlight the increasing regularity and number of incidents, the significant costs associated with such incidents and the potential exposure of Boards of Directors. In this publication, we look at some of the risks for directors around data breach incidents.

As businesses grow increasingly reliant on computers, the internet and the data that flows on these technologies, they also increasingly expose themselves to the risk of data breaches, being the intentional or unintentional dissemination of stored (and potentially valuable and confidential) information. Although these data breaches can occur unintentionally through poor business practices, many breaches today occur because of pre-meditated cyber-attacks.

Cyber-attacks (including theft, fraud, sabotage, espionage and hacking) are becoming increasingly diverse and sophisticated. Some indicators of the prevalence of cyber-crime include the following statistics:

- In 2010 and 2011 2.95 million cyber-attacks were detected in Australia; and
- Australian businesses lost an estimated $595 million from cyber-crime, with the cost of each data breach in 2011 being $2.16 million on average ($138 per compromised record). The goodwill costs to a business were on average $840,000 per incident in 2011.

Cyber-attacks and data breach incidents are also becoming of increasing public interest. For example:

- It is well known that in 2011 Sony's PlayStation Network was attacked;
- In October 2013, Adobe had a breach incident that resulted in user account information and, significantly, the source code of its Acrobat software being stolen; and
- In December 2013, retail giant Target was subject to a cyber-attack which caused a breach incident that affected 40 million credit card accounts and the extraction of the personal information of as many as 70 million customers (it has also been found that Target was just one of a number of United States (US) retailers hit by the attack).

These are only three of a large number of incidents. While some attacks aim to bring a company's IT systems to a standstill, many target valuable and confidential user and client information held by these IT systems.

Data breaches can leave directors and officers of the companies attacked vulnerable to civil suits (including class actions) for breaches of privacy legislation, corporate regulation or claims of misleading or deceptive conduct (for not adhering to the company's own privacy policy, especially in respect of IT security). To date the majority of the reported/public incidents and resultant actions against companies and their directors have occurred in Europe and the US. However, important lessons can be learned by Australian directors.

HIGH PROFILE EXAMPLES OF DATA BREACHES

Sony

Perhaps the most high profile example of a data breach in recent years was the attack of Sony's electronic systems back in April 2011. Hackers stole encrypted credit card details of 77 million users of PlayStation Network (owned by Sony) and the breaches cost Sony US $170 million. Some 1.5 million Australians and up to 280,000 Australian credit card numbers were exposed in the attack.

A month after the announcement of the breach, Sony's share price dropped 6 percent on the New York Stock Exchange because of a lack of consumer confidence. A significant factor in the drop related to Sony's perceived poor handling of the incident, including its inability to identify the full scope of the attack until seven days after it had occurred.

Sony's woes continued when upwards of 58 class-action lawsuits, primarily from the US, were launched against Sony and its affiliated companies. The United Kingdom (UK) Information Commissioner's Office (ICO) (the office responsible for upholding information rights and data protection) fined Sony $378,000 for a serious breach of the data protection laws.

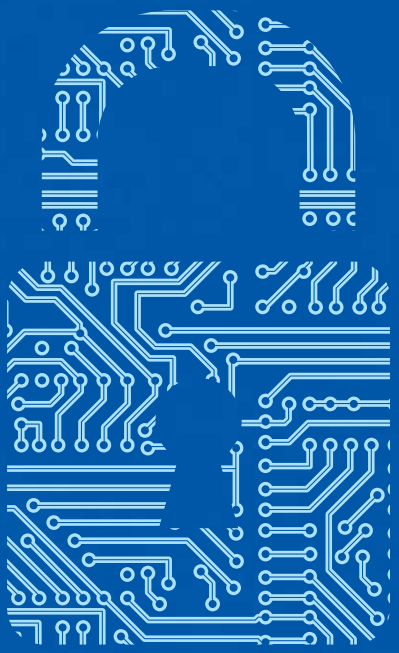
The lawsuits, which were commenced in various jurisdictions including California and New York, accused Sony of negligence and breach of contract for allowing the theft of personal data. The key issue in these cases was not whether Sony was liable but whether damages could be established.

The class actions were eventually dismissed. In doing so Courts in California and New York stated:

- Sony was not in violation of consumer-protection law because the named plaintiffs were receiving Sony's service without subscription;
- Sony admitted that the personal information was stolen as a result of the data breach but that did not mean Sony was any way involved with the data breach;
- No consumer was misled or deceived as users had signed Sony's privacy policy, which described Sony's security policy accurately; and
- The Court did allow leave for claims to be amended.

Adobe

In October 2013 Adobe was forced to announce that there had been a major breach of information they held relating to more than 3 million customers (including password identifying information). In the weeks following, Adobe admitted the breach actually affected more than 38 million accounts and also involved the theft of Acrobat source code (the building blocks of its Acrobat and Reader products). A password security firm has since confirmed that in all likelihood the data breach affected closer to 152 million customers of Adobe. If correct, this makes the Adobe breach the largest ever disclosed.



After announcing the initial breach, Adobe's share price immediately dropped 1.4 percent. (Interestingly, its share price recovered in the two weeks following the announcement.)

Although a sizeable portion of the 152 million accounts were considered to be fictitious, there is a reported concern that Adobe did not follow best practice for securing the password details of its customers (i.e. via a technique known as "salting"). Salting is the process whereby the company adds a secret code to every password after it is scrambled. This ensures that multiple encrypted versions of the same password are never the same making the encryption harder to decipher. More troubling is that the breaches were of information contained in Adobe's heavily promoted cloud platform, which is spread across numerous jurisdictions including the US, UK, India and Australia.

These alleged failings raised the possibility for legal action against the tech giant across multiple jurisdictions. Although (at the time of writing) only one civil action has been launched, Adobe is preparing for the worst in light of the actions that were brought against Sony and the enormous associated costs of defending them. Adobe may potentially be in a worse situation than Sony as its breach is larger and covers more jurisdictions than the Sony breach.

Target

In December 2013, Target disclosed that it had suffered a cyber-attack that resulted in around 40 million payment card numbers being stolen. However, similar to the Adobe incident, Target made a further announcement in January 2014 that stated that 70 million personal accounts data (names, contact details, etc.) had been stolen.

The Target incident is suspected to be the result of a "memory scraping attack." Visa had warned Target of similar incidents earlier in the year and had recommended various countermeasures. It is not clear if Target had implemented the countermeasures, but even if implemented they may not have been sufficient to repel the attack, which was more sophisticated than in previous incidents.

It is however suspected that Target's system was breached as early as November 2013, when attackers identified that Target's systems were "astonishingly open" and unsecure. This breach went undetected for many weeks by Target until it was informed of suspicious activity by the US Secret Service. Many interested onlookers await the US Securities and Exchange Commission's (SEC) determination of whether Target met the 2011 disclosure guidance guidelines, including in respect of Target's disclosures prior to the incident and also of its future disclosures.

Target has stated that its fourth quarter earnings had been hit by "meaningfully weaker-than-expected sales" since it disclosed the data breach and anticipated a 2.5 percent decline from its previous sales forecasts for the fourth quarter (noting that the announcement was only made in December 2013).

Target has been hit with more than 70 class action lawsuits filed on behalf of consumers and others. This includes at least two shareholder derivative actions against Target's directors and officers and the company itself regarding their failure to take reasonable steps to protect customers' personal and financial information from a potential data breach, and particularly their failure to implement any internal controls to detect and prevent a data breach. The actions also claim that Target, its directors and officers failed to provide prompt and adequate notice to customers and released statements that were meant to create a false sense of security to affected customers, which aggravated the damage caused.

While it is suspected that many of these actions will fail (particularly consumer based actions), there will be considerable interest to see how the various actions progress and in particular the shareholder based derivative actions given the circumstances surrounding the Target incident, the state of Target's security systems and their conduct following the breach.

THE AUSTRALIAN PRIVACY REGIME

While both the Sony and Adobe cases adversely affected Australians, under the previous privacy regime in place at the relevant times, it was difficult for an individual to bring a breach of privacy claim against either in Australia. While Australian corporations have been early adopters of online resources to maintain data, Australia has fallen behind the world in legislating how corporations deal with data breaches. Under the superseded legislation, neither Sony nor Adobe were required to report cyber-attacks, data breaches or breach of the *Privacy Act* to affected individuals or the Office Australian Information Commissioner (OAIC).

As of 12 March 2014, a consolidated set of principles called the Australian Privacy Principles (APP) now govern privacy and data protection throughout Australia (Federal agencies and the private sector) and significantly enhance privacy and data protection regulation and its enforcements. The APPs are the cornerstone of privacy protection in Australia and give the OIAC more powers in regulating how Federal public and private organisations handle personal information.

The OAIC has stated that a company will not necessarily have breached APP 6 (regarding unauthorised disclosure of private information) solely because a third party gains unauthorised access to information held by the company (via cyber-attack or otherwise). However, the OAIC's guidelines state that a company will have breached APP 11 (regarding the security of personal information) in such circumstances where it did not take "reasonable steps" to protect the information.

Significantly, the amendments to Australian privacy legislation gives the OAIC more and stronger powers to enforce adherence to the Australian privacy regime. These powers include:

- the ability to assess whether personal information is being handled in accordance with the APPs or relevant legislation; and
- the ability to apply to the Federal Magistrates Court to seek a civil penalty where an individual or company has breached a civil penalty provision of the privacy legislation.

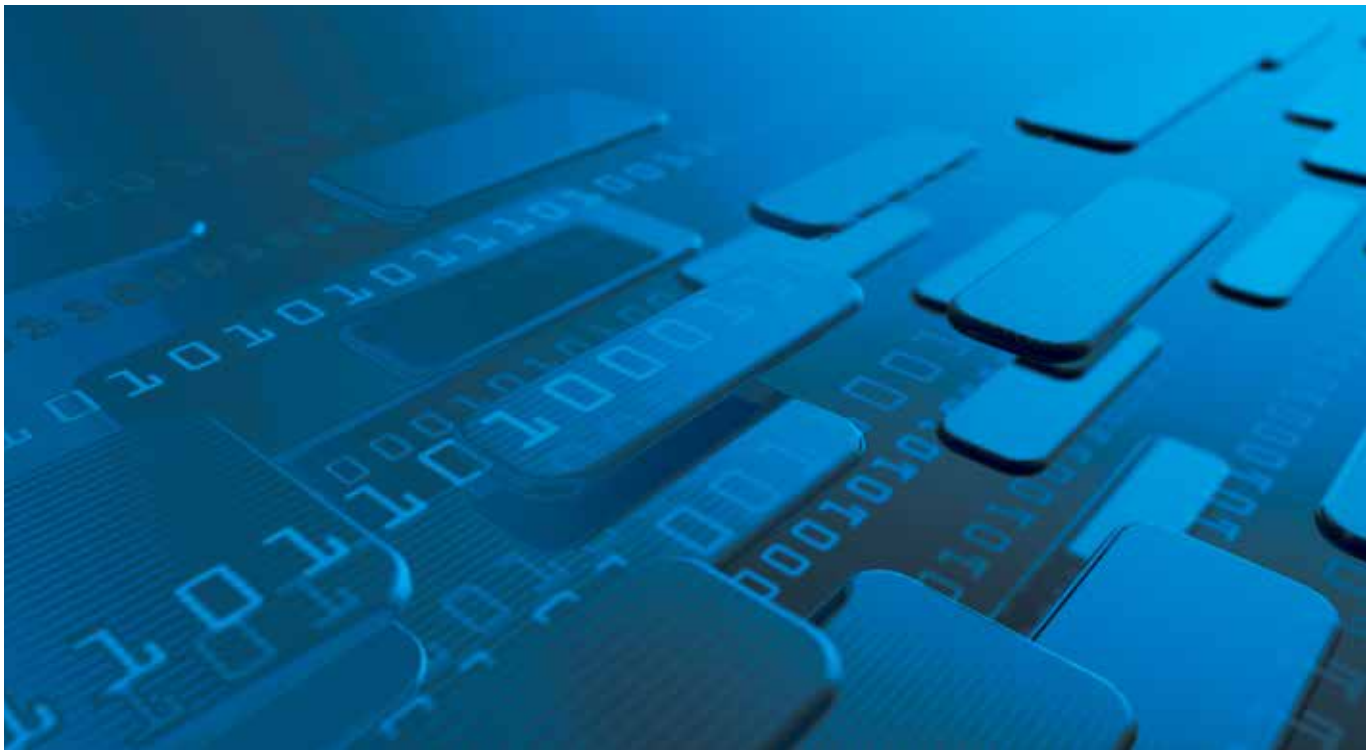
Corporate regulators also impose certain obligations on corporations and executives regarding data breaches. A company with an Australian Financial Services (AFS) licence, that is not regulated by the Australian Prudential Regulation Authority (APRA), must have "adequate technological resources" to provide financial services covered by the licence and "adequate risk management systems."

Whether technological resources are adequate will depend on the nature, scale and complexity of each business. However, resources will need to be sufficient to comply with all obligations under the law dealing with AFS licence holders, maintain client records and data integrity, protect confidential and other information and meet current and anticipated future operational needs.

APRA requires that businesses regulated by it have clear accountability and communication strategies to limit the impact of data breaches and have issued relevant prudential Practice Guidelines. APRA expects that businesses will notify it of any major security incidents. While these obligations are welcomed by Australian consumers, they only apply to a small number of Australian corporations and would not have been triggered in either the Sony or Adobe breach.

For comparison purposes we briefly describe the UK and US privacy regimes below.

THE UK SYSTEM	THE US SYSTEM
The main avenues in dealing with data breaches are through the EU Data Protection Directive 95/46/EC and *Data Protection Act 1998* (Act).	The US was one of the first countries where legislators (albeit at state level) passed legislation to mandate security breach notifications. The US has approximately twenty sector specific data security laws, as well as hundreds of similar State laws.
There is no mandatory requirement under the Act to report data security breaches. However, under the guidance notes issued by the ICO, if a breach affects a large number of people or is particularly serious, the ICO should be informed.	Forty six US states require residents to be notified of a security breach involving a person's name plus a sensitive data element (e.g. social security number, credit card or other government ID number that would permit access to a financial account).
The Privacy and Electronic Communications (EC Directive) Regulations 2003 requires public electronic communication service providers to notify the ICO of a breach.	Federal laws require notification of data breaches for health care information, information from financial institutions and breaches of government agency information. It is because data breach requirements are so evolved under US State and Federal legislation, that numerous proceedings against Sony were launched in the US and any likely claims against Adobe will also be brought in the US.



CURRENT ACTIONS TO ADDRESS CYBER RISK IN AUSTRALIA

Australia is attempting to "catch up" with the US and UK/EU and address its lack of governance on cyber risk issues. As discussed above, Australia has made certain changes to its privacy regime, in particular the APPs. Unfortunately, a Bill requiring mandatory data breach notification did not pass the Senate before Parliament was prorogued for the Federal election. Although the new Coalition Government believes in mandatory notification, they did not support the Bill (being the *Privacy Alerts Bills 2013* (Cth)) in its then form because of the Bill's perceived lack of due process and scrutiny.

Despite this stumble, it is inevitable that mandatory data breach notification laws will eventually become law and, as such, directors should watch with caution any future obligations regarding data notification. Current obligations regarding data breaches appear to focus on private and public entities rather than the actions of directors. However, that is not to say that directors could not be exposed to claims arising from such cyber-attacks. Other areas of law (discussed below), aside from the current privacy regime, may expose directors to liability in these circumstances. Further as the 2012 amendments to the privacy regime (which came into effect on 12 March 2014) encourage companies, and in turn directors, to disclose breaches, directors should seek to confirm that such systems are already in place and are up to standard.

ARE AUSTRALIAN DIRECTORS CURRENTLY AT RISK FOLLOWING A DATA BREACH?

Despite the lack of specific obligations regarding data breaches for directors (at this stage), they may nevertheless face exposure. Current common law and statutory duties imposed on directors in Australia may, in our view, be interpreted to apply to data breaches in certain circumstances. Directors should have particular regard to their duties of continuous disclosure and the duty of care and diligence under the *Corporations Act*. Although, as we far as we are aware, these duties have not yet been considered by an Australian Court specific to the area of cyber security it is, in our view, possible that such obligations could be used to bring actions against directors.

In the *Centro Case* directors were found to have breached their duty of care and diligence by not disclosing an obvious error in the company's financial statements. The Court in *Centro* said that the approval of financial statements was a key element of corporate governance and could not be delegated. In particular, a director cannot escape his or her duty of care and diligence where certain errors were so obvious "Blind Freddy" would have seen them. Although the *Centro Case* related to a company's financial statements it is possible that this ruling could be adopted to different scenarios, including key issues of risk management. We expect that cyber security and data integrity will increasingly become a key consideration of many corporations' risk management strategies. In that context directors, in the discharge of their duties of care and diligence, will be expected to assume responsibility for adequate risk management policies including security and data integrity.

All Australian companies listed on the Australian Securities Exchange (ASX) are under a general obligation to inform the ASX of any information that a reasonable person would expect to have a material effect on its price or value. It is not clear at this stage whether a reasonable person would expect a data breach to affect the value of the company all the time as it did in recent high profile cases (such as the Adobe case). In this respect, current research indicates that in nine out of ten occasions where data breach has occurred, a company's share price is not affected.

However, it is arguable that any share drop, including a short term "blip", is material. As the Sony case demonstrates, there is a risk that any data breach could negatively affect share price. In this respect, it will be interesting to see what litigation will flow from the Adobe breach that resulted in a small short term drop in share price. Ultimately, whether a data breach is a material matter for disclosure purposes will depend on the type of company, the nature of its business and the extent of the breach. For example, the share price of a company that deals with highly sensitive financial information and is heavily dependent on online business may be more vulnerable to a data breach than others. Ultimately, it will come down to the facts of each case. Further, as the law develops and the public becomes more sensitive to data breaches, the impact on share price may become more pronounced. Directors should therefore very carefully consider when they should make disclosures to the ASX of data breaches so as to avoid breaching the *Corporations Act* and minimise the chance of potential class actions by new or existing shareholders.

Australian directors should carefully adhere to their duty of care and diligence. A director is required to discharge their duties with a degree of care and diligence that a reasonable person would exercise in their position. This would include, as the *Centro Case* demonstrates, monitoring and reviewing a company's risk management and data security policies.

In determining whether a director has satisfied this duty, the Court will balance the foreseeable risk of harm against the potential benefits that could reasonably have been expected to accrue to the company from the conduct in question.

Such obligations, when applied to the risk management (including data protection) elements of a company, would suggest that a director could be found liable for data breaches, if they failed to put themselves into an informed position to guide the company's position on cyber-security.

Actions against Australian Directors

The above highlights that Australian directors may be exposed to actions (including class actions) as a result of data breaches. Such actions could come from either the corporation's shareholders or customers. It is worth bearing in mind that directors and companies should not simply be concerned about damages awarded against them in proceedings, but also the associated costs involved regardless of the outcome of a claim. These include a lower share price, reputational damage and the massive costs in defending the proceedings. As the Adobe case shows, these disputes will often have a cross jurisdictional element which would further increase the complexity, costs and risks.

Under derivative action provisions in the *Corporations Act,* shareholders could bring proceedings against directors if it is in the best interests of the company to do so. Derivative action has often been seen as an effective tool to make directors accountable for their actions.

While no derivative actions have yet been brought in Australia for data breaches, directors should be cautious. Empirical evidence suggests that 51 percent of all derivative proceedings tend to be brought against directors for breach of their duties, as opposed to claims relating to breach of contract, oppressive conduct and debt recovery. Such figures, coupled with shareholder activism and the active litigation funding industry, should make directors wary of the risk of data breaches. It is foreseeable that the increase of personal information held by companies and the potential for attacks on this information could create a perfect storm for litigation against directors.

Shareholders, and potentially customers, who have purchased shares or products and relied on a company's risk management and data protection system to undertake such a transaction, may have recourse to launch proceedings against companies for data breaches, as a litigation strategy recently used in California. The strategy involves shareholders or customers using misleading or deceptive conduct legislation (in Australia this would most likely be under the *Australian Consumer Law*) to bring proceedings against companies that do not implement their own privacy or risk management policies properly (or at all). Under the *Australian Consumer Law* directors may be found personally liable for the misleading and deceptive conduct of a company if they are found to have "aided or abetted" or otherwise "been in any way, directly or indirectly, knowingly" involved in such conduct.

In California, plaintiffs have begun to argue that if, in a privacy policy, a company says it takes reasonable steps to protect information then that company must take reasonable measures to protect the information of its customers. As such, if the OAIC found a director did not implement industry best practices for protecting its data from potential breaches under APP 11 (see above), a plaintiff could potentially bring a case against the company, arguing its privacy or risk management policies were misleading. Under such proceedings, in a case such as the Adobe one, plaintiffs may argue the company is liable for failing to follow best practice in protecting its customers' passwords.

However, in other jurisdictions where shareholders and customers could bring (and have in other jurisdictions brought) claims against directors, these groups first need to show that a director's (or company's) actions have caused them actual harm. For example, a customer whose personal information may have been stolen because a company failed to implement its privacy policy would need to prove this caused them a real injury. This requirement may be satisfied if the customer were a victim of actual credit card fraud (or other tangible loss). Customer class action suits (such as Adobe or Target discussed above), relating to data breaches, need to establish that the customers suffered an actual loss.

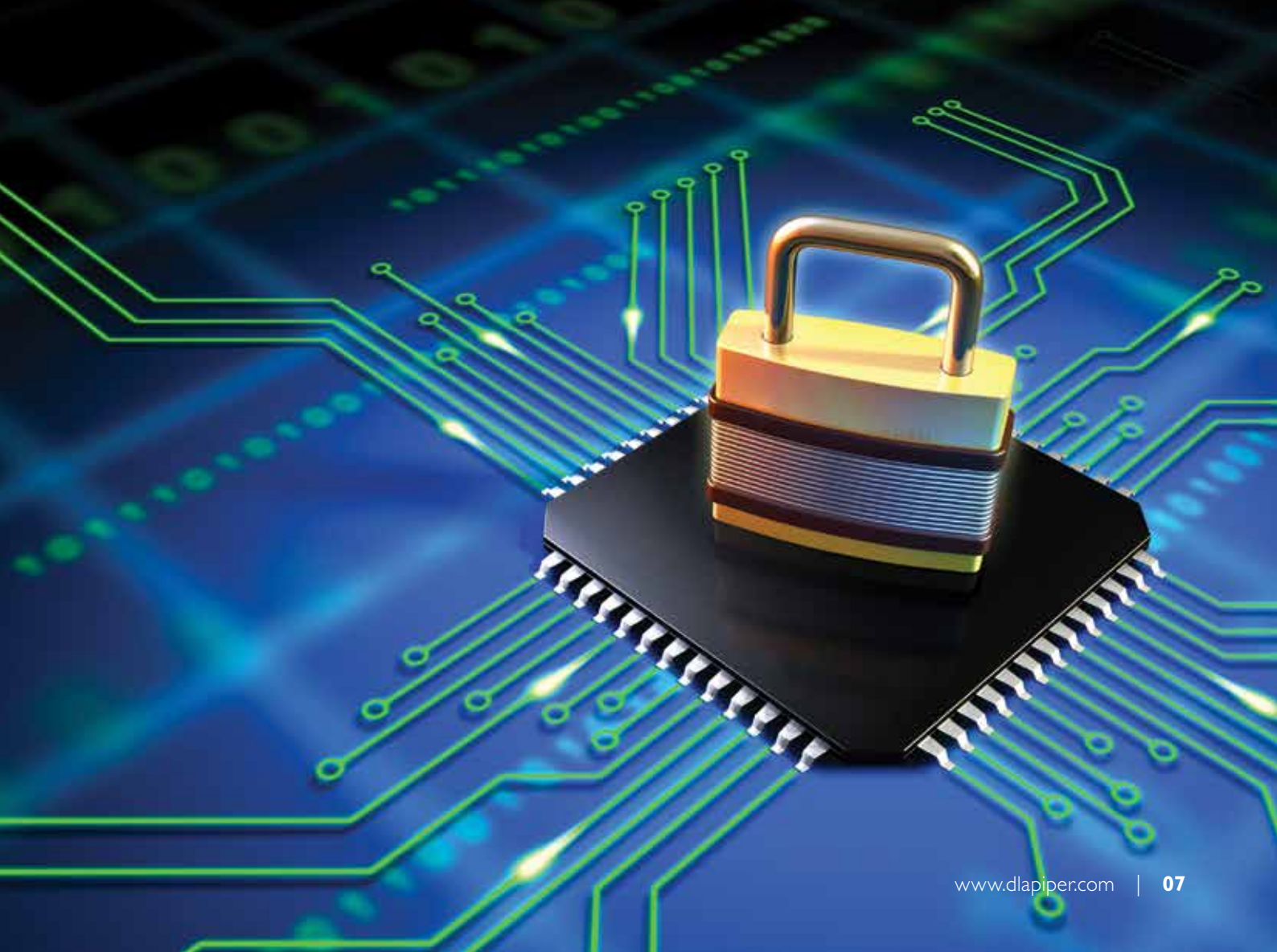
In our view, it is only a matter of time before these types of arguments are tested in Australia, particularly by shareholders of companies who, depending on the nature of the company, might find it easier to show a loss. As such, it would be prudent for directors to implement effective risk management policies and place a heightened emphasis on ensuring appropriate cyber policies and privacy policies are in place and correctly implemented.

CYBER SECURITY AND THE DUTY OF CARE: A CHECKLIST FOR BOARD MEMBERS

To properly address the rising concerns about cyber risk, directors must start to ask the following questions:

- ☑ Who is in charge of cyber security within the company? Are there checks and balances by having the duties divided between relevant teams (i.e. the privacy officer and the information security officer) and what role does Board oversight play? In particular, in respect of Board oversight, there should be a director who takes the lead on/ responsibility for information security (whether informally or formally).
- ☑ Has the company mapped the network (i.e. IT system network) against information security functions and protections, identified the likely external and internal threats and the interplay between physical and cyber security? In particular, if the company has programs such as BYOD (i.e. Bring Your Own Device), what are the policies and safeguards applied to such devices and how does the company ensure that the policies are implemented in practice?
- ☑ What is the company's incident response plan and how well is it disseminated through the organisation? Does it cover all the matters (including regulatory notifications) that it should cover? In addition, practical matters such as how to communicate with all relevant stakeholders, including customers and suppliers, should be included.
- ☑ Finally, what insurance does the company carry for cyber security and data privacy breaches? Is it an up-to-date policy and does it cover the matters identified as part of the network and threat mapping? What are the policy limits and exclusions on the insurance coverage? In particular, is it a purpose built cyber security and privacy breach policy that fully covers the company or is it simply an *"add on"* best fit available ad hoc addendum to an existing policy?

Ensuring the above questions are properly addressed will go a long way to protecting companies and their stakeholders, whilst also protecting directors.



CONCLUSION

Despite a company's best endeavours, it is inevitable that data breaches will occur. In light of this it is vital that directors implement appropriate risk management and data protection systems now. Although such actions may not stop cyber-attacks from occurring they will go a long way to limiting the potential damage that will be caused to a company by these attacks, while also ensuring that directors are adequately insulated against potential actions arising in this field.

www.dlapiper.com