COMPUTERS & LAW

Journal for the Australian and New Zealand Societies for Computers and the Law

Editors: Daniel Thompson, Isaac Lin, David Ng, Moses Kakaire ISSN 08117225

Number: 89 September 2015

"The big print giveth and the small print taketh away"

Assessing cyber security risks and the role of cyber insurance

By Dudley Kneller and Koula Politis

***Dudley Kneller** is a partner with Madgwicks Lawyers*

***Koula Politis** is a lawyer with Madgwicks Lawyers.*

1. Cyber security breaches – closer to home than you think

Most people associate "cyber breaches" with criminal hacking, political "hacktivism" or sovereign state espionage. These types of cyber breach events are newsworthy, seem to happen overseas more often than not and attract broad media attention. They seem quite removed from the world of the average business in Australia.

Consider the cyber attack on Sony Pictures in November 2014. This cyber attack wiped out approximately two-thirds of Sony Picture's computer systems and servers and was reportedly one of the most destructive cyber attacks ever to take place on American soil.[1] Speculation that North Korea was behind the attack quickly surfaced with a direct link to Sony's controversial new comedy *The Interview*. Ultimately the incident culminated in the United States imposing sanctions on North Korea in response.[2]

Cyber breaches do not just happen overseas however. Australian organisations too are increasingly likely to suffer from cyber breach events without necessarily experiencing any of the Hollywood fanfare.

In this issue

Dudley Kneller and Koula Politis: "*The big print giveth and the small print taketh away*" Assessing cyber security risks and the role of cyber insurance 1

Andrew Jaworski: Update: Recent Online Anti-Piracy Reform In Australia" 7

Sylvia Song: Privacy and criminal records Comparing the British and Australian experience 11

Kevin Chen and Christopher Chiam: An essay on the culpability of supporters and 'Likers' in instances of cyber bullying 15

From the editors…

In this issue, Dudley Kneller and Koula Politis discuss the threats, risks and impacts of a cyber attack on the average Australian business and consider the market for cyber security insurance.

Andrew Jaworksi considers the Government's response to the prevalence of on-line piracy. This includes recent amendments to the Co*pyright Act 1968* that have made it easier for rights holders to block content hosted on foreign websites and the proposed *Copyright Notice Scheme Code 2015* which provides for warnings to be issued to individual consumers who unlawfully downloaded copyright material.

Sylvia Song contrasts the treatment of criminal records in Australia and the United Kingdom to explore the inherent conflict between an individual's right to privacy and the public interest in crime in the community.

Finally, Kevin Chen and Christopher Chiam argue for tougher criminal legislation to deal with cyber bullying. They propose additional regulation to cover social media users who 'like', 'share' or 'comment on' harmful content.

The Editors

Daniel Thompson, Isaac Lin, David Ng and Moses Kakaire

With increasing awareness of cyber security issues there is now a variety of information available which provides organisations with advice on how best to combat the risks of cyber security breach events. There is little information however on whether cyber insurance products should form part of your risk mitigation strategy. This article briefly explores the rise in cyber security breaches before discussing the role cyber insurance products can play in mitigating risks in this area.

2. How do cyber security breaches occur?

Before examining the topic in any detail it is helpful to understand first how such breaches can occur in the first place. There are 3 main ways that cyber security breaches can occur: Firstly, as a result of a criminal and/or malicious attacks (i.e. hacking), secondly, through the negligence or mistakes of employees or contractors, and finally as a result of technology or system failure.[3]

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.

It is clear that businesses need to consider how to design their systems security and access regimes to minimise the risk of unauthorised access to company data and prevent the occurrence of security breaches – both from "within" and "without".

Being adequately prepared will enable you to be in a better position to respond rapidly to a cyber event, to control and manage the subsequent impact on the business and to effectively manage any brand or reputational fall out. Having a plan in place will ultimately save your business both time and money.

3. What are the real risks?

The most obvious risk to your client's business is the loss of commercially sensitive information such as the loss of trade secrets or disclosure of personal information. Laws relating to breach of confidentiality are well established. The remedies available for breach include taking action to try and compensate for the loss and damage suffered by such breach, although damages are not always an adequate remedy.

It is well known that once confidentiality is lost it cannot be regained so it is important to take necessary preventative measures to properly protect and secure information.

If the Privacy Act 1988 (**Privacy Act**) applies to your organisation, you 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. These include fines of up to $340,000 for individuals and $1.7 million for corporations as well as the potential for compensation orders to be awarded.

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. Directors should consider the risk of shareholder litigation against the board if there is a risk 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.

Another risk area involves security breaches or outages that result in systems crashing and the loss of a business' online presence. If a trading entity's website is down or if employees cannot access the network, the business is at risk of losing the online business generated by traffic

to its websites as well as the loss of productivity when staff cannot access systems.

Civil litigation risk can pose particular risk. We are seeing greater incidence of class action litigation in the United States flowing from large scale data security breaches. Notable cases include litigation following the Target breach and the Sony Playstation breach.

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, business continuity, privacy or breach of confidentiality. Contractual agreements may result in companies being liable for damages claims for a breach of these contractual obligations that might be caused by a cybersecurity breach.

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

4. What are the financial impacts of a cyber security breach event?

The financial costs of a cyber attack or a cybersecurity breach 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 reflected in revenues or relates to projected losses. On the other hand the costs and expenses associated with public relations and marketing campaigns to restore brand and goodwill are business expenses that can be measured.

In 2013 the average cost of a data breach for each compromised record was estimated at $141 per record.[4] The Ponemon Institute published its global analysis study of the cost of data breaches in 2014. The study revealed that in 2014 the average cost to a company of a data breach increased by 15 per cent on the previous year.[5]

Some costs occur almost immediately following an event. The costs associated with responding to an event and remedying the breach are generally easy to identify. A business will often need to bring in external advisers including lawyers, technology advisers and other experts to assist from the early stages.

Once the breach has been initially managed the task of identifying affected parties including staff, customers, suppliers and other third parties begins. You will need to consider how best to communicate with these affected parties and there are clearly costs associated with this activity. For larger breach events involving hundreds or even thousands of affected individuals it is not uncommon to see dedicated call centres being established in order to properly notify the impacted parties. These call centres are often set up to not only deal with initial communications but to deal with subsequent follow up activities including managing refunds or claims where applicable.

Don't forget other "interested" parties including regulators such as the Information Commissioner and any other applicable regulators will all expect to be informed of any breach event occurring within your organisation. You will typically need to appoint advisers to properly understand who these parties are and the level of disclosure and information required. You will also need to know what potential civil penalties are available for serious or repeated data breaches involving a breach of the Privacy Act and the potential liability for compensation awards being made.

The costs don't just stop there. Following initial notification activities you are likely to need ongoing assistance with putting in place steps to ensure the breach does not occur again in future. This involves appointing technology and forensic advisers to assist with new and improved security measures, penetration testing activities and associated governance and policy development.

The costs associated with business interruption are often underestimated. When your business cannot trade effectively and your people are unable to carry out day to day work functions and activities the cost is likely to be considerable.

As you bring the breach under control and begin to restore operations you will of course be trying to minimise the PR fall out to protect your trading reputation. Many businesses who have been impacted by cyber security breach events struggle to manage this external "comms" piece. Often communication to the market, media and other interested parties comes too late following the event or is inaccurate. Follow up communications are sometimes sporadic and many organisations underestimate the amount of work involved in effectively managing this part of the situation.

Reputation and brand management is critical to get right. More often than not external consultants will be able to advise you on appropriate steps to minimise damage to reputation. They can assist with an appropriate PR and marketing campaign to get the business back on its feet and demonstrate that you are again "open for business".

This type of PR campaign is aimed at mitigating future losses by stemming the flow of lost trade revenues - the campaign shows the market that the business is better equipped and can be trusted again in the future.

5. Mitigating the risks?

It is not possible to avoid all risks. In an environment of rapid technological advancement and reliance on networked communications and IT systems, it is

inevitable that breaches will occur and that the sources of cyber security threats will continue to be ever changing.

What the regulators say

In 2014 the Office of the Australian Information Commissioner (**OAIC**) published guidelines relating to data breach notification[6] and in January 2015 it published new guidelines on 'taking reasonable steps' to securing personal information[7].

The OAIC guidelines provide a useful insight into the regulator's approach to the responsibility of business for information security generally and to compliance with the Privacy Act. 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 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.

In March 2015, the Australian Investments and Security Commission (**ASIC**) released a report titled *Cyber resilience: Health check*.[8] Australia's corporate regulator is intending to play a greater role in improving the cyber resilience of regulated entities and intends to incorporate cyber resilience into its surveillance activities.

ASIC has identified regulated 'licensee' entities as having particular legal and compliance obligations that may require them to review and update their cyber risk management practices. For ASIC's purposes, regulated licensee entities cover a variety of entities licensed under applicable corporations law and includes Australian financial services licensees (AFSL). ASIC has also endorsed the *US National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity* (NIST Cybersecurity Framework) as a useful resource for regulated entities and has indicated that this resource will be of particularly relevance for licensees.

So what can I do about this?

Being prepared is key to managing and mitigating risks relating to cybersecurity breaches. It is impossible to achieve absolute prevention but there are steps you can take to increase the security measures in your business to help avoid the financial impacts of breach events and to comply with the requirement to take reasonable steps to protect and maintain information and the security of your network.

Part of that process involves giving thought to mitigation strategies and to managing damage once it occurs. But the first step is developing a culture of compliance and cybersecurity awareness. This will require that senior management takes an active role in undertaking a comprehensive analysis and assessment of the cyber risks that are relevant to your organisation and to assess the adequacy of existing cybersecurity measures and processes.

You should understand your organisation's critical infrastructure and vulnerabilities which will enable you to properly determine what steps are needed to mitigate the risks. You may need assistance with reviewing your cybersecurity risk and response capabilities periodically to ensure that you are keeping up with developments in the regulatory environment.

With an increasing awareness of cyber related issues there is no shortage of materials available to assist you to address cyber security risk events. This article now looks specifically at cyber insurance as a legitimate risk mitigation strategy.

6. Cyber insurance cover – some of the background and basics

What has been a growing trend overseas has now reached Australian shores with companies now turning to specific cyber insurance policies to cover themselves for losses in relation to cyber breach events. A leading global cyber insurance provider has said that developments in technology have created new exposures that organisations did not face as recently as five years ago. It pointed to cases going through the courts where "insurers are denying coverage rather than willingly paying for a large catastrophic loss [unless they have specific cyber insurance]."[9]

As a result cyber insurance policies are playing a bigger role in mitigation strategies. A review of your cybersecurity risk profile will assist you to assess whether your business should consider a separate cyber insurance policy for itself as well as possibly also imposing obligations to obtain this type of cover on your third party vendors.

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.

Typical cyber insurance policies cover the following risks:[10]

- unauthorised access to or use of physical or electronic data within a computer network or the business;
- network outages, viruses, malicious code, computer theft or extortion;
- business interruption;
- costs of notifying breaches; and
- costs of responding to regulatory investigations.

Cyber insurance policies will have different requirements to standard business insurance policies so it is important to ensure you access brokers and insurers who specialise in the area.

7. What to look for in a cyber insurance policy?

Cyber insurance coverage is generally conditional on organisations having adequate security systems and risk management strategies in place. In some instances it can be quite difficult to obtain and policies are becoming increasingly costly. Cyber insurance should be seen as an additional tool for organisations and part of a holistic approach to managing data breaches and technology risks. Organisations won't be able to simply rely on cyber insurance without putting appropriate security practices and procedures in place to avoid breaches in the first instance.

We have recently seen the entry of two Lloyd's of London backed insurers Beazley Group and CFC Underwriting Limited both announcing the introduction of data breach insurance in Australia. These insurers join a market place dominated by traditional insurers such as Allianz and AIG who also have various policy options available.

8. Some watch outs for businesses looking to take up a policy include the following:

- Carefully consider the policy terms and conditions. This generally goes without saying but "*the big print giveth and the small print taketh away*".
- Often policies will impose minimum security requirements before offering any sort of coverage. You can expect to be "qualified" by the insurer who will want to confirm you have adequate security controls in place to begin with.
- Are there any steps you can take from a security perspective that may give the insurer additional comfort and more importantly reduce the premium? If so what are they, how can you implement such steps and at what cost?
- What ongoing audit and compliance obligations do you have to undertake to ensure the policy remains current and will respond appropriately? Some insurers will expect a level of ongoing reporting and reserve the right to audit your systems and security protocols in place.
- Ensure you are very clear on your role in the event of a security breach incident and how this ties in with your insurance obligations. Getting this right may be the difference between the policy responding or not.
- Beware policies which only respond after a minimum downtime period. Cyber security breach events once triggered happen very quickly. You will not want to have to wait 12 hours or 24 hours before you are able to call on the protections in your policy to assist – by then it may be too late.
- Your insurer and broker are often a good source of information and best practice and may be able to refer you to subject matter experts who can assist with putting in place adequate security protocols, cyber compliance programs or undertake penetration testing to assist the you to get up to speed.
- How does the policy fit with your existing insurance coverage – beware any overlaps or more importantly "gaps" between policies which will leave you exposed?
- Technology is evolving so fast and hackers are generally at the forefront picking up on new vulnerabilities and opportunities to ply their trade. Make sure you understand how the policy evolves over time to pick up and include additional risks as they become apparent. What does your insurer do to enable the policy to remain "ever green"? Is this something that happens once a year or is it ongoing? What is the associated cost of amending the scope of the policy and will there be new exclusions which come with this change in scope which may impact your business risk profile?
- Understand the impact on your premium and any additional obligations which are likely to be imposed in the event you need to make a claim. Are there any benefits in not making a claim – will this reduce your premium at all?
- Does your insurer understand your industry and any unique regulatory requirements which may apply. If in the regulated space we would expect you to have ongoing discussions with your main regulator to make sure it is aware of any relevant standards or other best practice which the regulator expects to be covered off. Make sure your broker and insurer understands any industry "nuances" which may affect the policy.
- Often breach events take months or in some cases years to discover. Be aware of any applicable exclusions and ensure you understand what happens in this situation. It may well be that your policy has expired. Some insurers will allow organisations to pay an "optional extended reporting period premium" to provide additional time in which you can notify of a claim arising during the period of the policy. This optional period is generally no more than 12 months however, so may not pick up on these "sleeper" events.
- Insurers will typically not provide insurance cover for any action for damages brought in a court outside the policy's specified territories. It is therefore crucial to ensure you are aware of any territory limitations which may apply to your policy and if they conduct business outside Australia how claims affecting these interests will be impacted.

With such a long laundry list of issues to consider, cyber insurance policies are not to be considered lightly. However, with cyber breach events on the rise and with technology forming such an integral part of Australian business, cyber insurance coverage is increasingly likely to form part of your strategy to combat this risk. Your customers, suppliers and regulators will no doubt be expecting you to be up to speed with the latest developments.

COMPUTERS AND LAW JOURNAL

2015 STUDENT PRIZE - $1,000

for the best article in the field of computers and the law.

The Computers and Law Journal for the Australian and New Zealand Societies for Computers and the Law offers a prize of AUD 1,000 for the article which is selected by the editors of the Journal as the best article in the field of computers and the law written by a student.

Final closing date for applications for the prize is: **9 December 2015**.

Articles must be no more than 1500 words and must be submitted online with an appropriate covering message to:

editors@nswscl.org.au

In the covering message, applicants must provide details of their candidature, including the name of the educational institution at which they are enrolled and their student number.

Submissions for the student prize will be assessed by reference to the following criteria:

- new or innovative content, for example new case(s), new law, new technology dealt with or used in law or in legal practice, or innovative review of perspectives on computers and law;
- research competence, including proper referencing of all authorities used;
- well organised for communication of points; and
- clear points and objective.

The winning student will receive a prize certificate as well as $1,000, and the winning article will be published in the next edition of the Journal as the winning article; the winning student will also receive a free copy of the Journal edition in which the article is published. The article will be published online at the website for the NSW Society for Computers and the Law at: http://www.nswscl.org.au/journal/

The editors reserve the right not to award the prize. It is intended that the prize be offered annually but terms of the offer may be varied.

The Computers and Law Journal reserves the right to publish articles submitted for the prize which are not the winning article. Applicants will be advised if their article is to be published; they will receive a free copy of the Journal in which their article is published.

Articles may be co-authored as long as all co-authors are students and there are no more than 5 co-authors. If they win, co-authors will be paid the prize in equal shares but they may redistribute their shares by their own agreement. Initial format for articles is the same as for all articles submitted for publication by the Journal; details of this format are available at: http://www.nswscl.org.au/journal/contribute.htm

STUDENTS ARE NOW INVITED TO APPLY FOR THE PRIZE.

Submitting an entry is a warranty that the student has the right to publish in the Journal.