sparke HELMORE LAWYERS

Cyber Update

OCT 2022 ISSUE 1

IN THIS ISSUE

Jehan Mata

Partner
Sparke Helmore

Welcome to the first issue of the Cyber Update, a new publication providing you with a selection of essential updates on the fast-paced world of cyber, aimed at keeping you at the forefront of issues and legislative changes and impacts.

In this issue, we focus on national and international cyber topics relevant to industries and businesses, including supply chain (third party) attacks, how cyber incidents can affect critical infrastructure, and how cyber criminals capitalise on natural disasters, warfare and changing political and economic landscapes. This issue also features a special update from New Zealand firm Duncan Cotterill (a fellow member of our Global Insurance Law Connect network) on the New Zealand cyber space.

The topics covered in this issue of the Cyber Update are:

- Cyber-attacks on critical services: around the grounds
- Natural disaster, warfare and the changing political and economic landscape: the impact on cybercrime
- The changing face of the legislative landscape
- Our take on *Inchcape Australia Ltd v Chubb Insurance Australia Limited* (2022) FCA 883.
- DIY Insurance: are captive insurers the future of cyber insurance?
- Supply chains: you are only as strong as your weakest link.
- Who is accountable for cybersecurity?
- Current trends of cyber risk in New Zealand – The role of risk management and insurance.

We hope you find this issue informative and useful. If there are any topics you would like us to cover in future, please contact Jehan Mata.

CYBER-ATTACKS ON CRITICAL SERVICES: AROUND THE GROUNDS

Author: Partner Jehan Mata
Acknowledgment: Georgia Mineo and Noor Klank

Cyber-attacks on critical infrastructure can cause significant harm to an organisation directly but also to individuals. In this article we discuss the attacks on critical infrastructure in the past six months and the ramifications of these attacks and also highlight the importance of organisations taking the necessary steps to put appropriate procedures in place to mitigate and manage the risk of a cyber-attack.

Health sector

Over the last decade there has been a move toward centralisation of information on digital platforms, especially in the health sector, aimed at ensuring the continuity of treatment. However, with every system comes vulnerabilities and therefore it is essential for critical organisations, such as those in the healthcare industry, to have appropriate procedures and systems in place to mitigate and where possible avoid the risk of a cyber-attack. According to the most recent data from the Office of the Australian Information Commissioner, health service providers remain the top sector to notify data breaches.[1]

It is feared that a state-sponsored cyber-attack on 4 August 2022 was the cause of the shut down to the United Kingdom's, National Health Service's (**NHS**) crucial service, NHS-111. This came after the Five Eyes International Intelligence Alliance warned of malicious cyber activity in response to the United Kingdom's position on Russia's invasion of the Ukraine. All NHS trusts were forewarned of the potential attacks and were cautioned to shore up essential cybersecurity systems and ensure back-ups were in place.

NHS-111 assists people with getting the right advice and treatment when they urgently need it. Consequently, patients were left struggling to get urgent appointments and ambulance callouts. The attack relegated NHS-111 staff to "working on paper", which negatively affected response times to patients needing urgent care, the ability to book patients directly for appointments and provide

[1] Office of the Australian Information Commissioner, Notifiable Data Breaches scheme 12-month insights report, Commissioner's foreword (13 May 2019) <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-scheme-12month-insights-report>

emergency out of hours prescriptions. A ripple effect of this alleged attack caused the NHS to run at unsustainable levels with long delays in emergency departments, staff shortages and a lack of beds.

NHS-111 was not the only health service impacted. Caresys—a care home management software used by more than 1,000 homes across the United Kingdom—was targeted; as well as Carenotes, a patient record management system used by 40,000 clinicians, which was subsequently shut down.

This is not the first time that this type of attack has crippled the NHS. In 2017, the NHS was impacted by a global ransomware cyber-attack, dubbed "WannaCry". Over 600 organisations that provided acute care, specialised medical services, mental health care and ambulance services were affected. The service providers were either locked out of digital systems and medical devices (such as MRI scanners) or had systems disrupted. Like the recent attack, staff were forced to revert to manual processes, appointments and surgeries were cancelled, emergency telephone service response times were delayed, and emergency ambulances were diverted to other hospitals. The attack lasted for four days and resulted in significant financial impact of GB£35 million, not including the unreported human cost.

Aside from this instance, the largest cybersecurity attack ever experienced occurred in 2015 and hit the Anthem Blue Cross Insurance System (health insurer) in the United States. There was an unauthorised access of consumer information, including member's health identification numbers and social security numbers. Cyber criminals gained access to the system via spear phishing, which revealed usernames and passwords. Over 78 million people were affected by the attack and Anthem had to pay approximately US$40 million in settlement.

Similarly, in Singapore a major cyber-attack occurred and over one million patient records, including the Prime Minister's records, were stolen from SingHealth, Singapore's largest health group. The medical records contained financial information, health details and social security information and as a result of the breach, SingHealth and its technology subsidiary were fined SG$1 million, the largest privacy fine in Singapore's history.

Transport sector

The transport sector has also been impacted by cyber-attacks in 2022. On 24 March 2022, Trenitalia and Ferrovie dello Stato, the companies that operate rail transport in Italy, were affected by a ransomware hacking. A US$5million Bitcoin ransom was requested to be paid within three days of the attack for the system to be unlocked. If the ransom was not paid, it would increase to US$10million. The attack caused major disruptions to the purchase and sale of tickets.

On 4 June 2022, ransomware attackers targeted the Cape Cod Regional Transit Authority servers in the United States. While the bus route was unaffected, the Authority's "Dial-a-Ride" Transportation bus service, which allows users to schedule a ride 24 hours in advance, was impacted. On 3 August 2022, in a more unique and less-purposeful attack, hackers were able to manipulate an electronic display at a station on the Wuppertal Suspension Railway in Germany and display pornographic content.

Energy sector

Since 2017, and with the escalation of geopolitical tensions in parts of the world, oil assets and infrastructure have emerged as one of the biggest targets for cybercriminals. The largest ransomware attack on an oil supplier occurred in May 2021 in the United States. Major oil supplier Colonial Pipeline was targeted, which saw supplies tighten across the country and multiple states declare an emergency. In response to this attack, and noting the real risk of being targeted again, particularly in the current political climate, President Biden signed an executive order to improve cyber-defences.

More recently, in February 2022, IT systems were disrupted at Oiltanking in Germany, SEA-Invest in Belgium and associated ports in Africa and Evos in the Netherlands. The attack disrupted the port supply chains and slowed the delivery of oil shipments. In July 2022, Ukraine's biggest private energy firm, DTEK Group, that owns coal and thermal power plants in various parts of Ukraine, was also the victim of a cyber-attack. The attack attempted to destabilise technology and spread propaganda about the company's operations.

Since these two attacks, 18 global companies from the oil and gas community have followed warnings from governments about the risk of attacks and have taken a cyber resilience pledge at the World Economic Forum Annual Meeting 2022.

Financial sector

In a more recent incident, on 11 August 2022, Malaysia sustained a cyber-attack on its payment gateway, iPay88 (the **Company**), that offers comprehensive payment methods to companies, which include e-commerce and retail solutions. The breach originated from and was confined to the Company's payment card systems with customers' card data being compromised. The Company noted that it had discovered the breach on 21 May 2022 and immediately initiated an investigation and brought in the relevant experts to contain the breach. As a result of the attack, the Company implemented various new measures and controls to strengthen its system's security. The investigations remain ongoing and the ramifications of the attack are yet unclear.

Prevention is better than cure

Cyber criminals do not discriminate, cyber-attacks are a global issue and critical infrastructure remains a prime targets for cyber-attacks.

We have provided a very brief snapshot of a few of the notable attacks and the impact of those attacks on organisations and businesses as well as individuals. What is abundantly clear is that even the most advanced industries are vulnerable. Looking at the health sector alone, the incidents referred to highlight the severity of consequences arising from a cyber-attack, which can directly impact the health of individuals.

The motto is "*prevention is better than cure*". Organisations must take the necessary steps and have the appropriate procedures to mitigate and manage the risk of an attack as being on the receiving end of an attack is inevitable and the ramifications are not only detrimental financially but, can also result in significant reputational damage causing loss of public confidence and worst, result in a life threatening situation.

NATURAL DISASTER, WARFARE AND THE CHANGING POLITICAL AND ECONOMIC LANDSCAPE: THE IMPACT ON CYBERCRIME

Author: Partner Jehan Mata
Acknowledgment: Georgie Aidonopoulos

The frequency of cybercrime has been steadily growing in recent years. A key factor in the increase of successful cyber-attacks is that cyber criminals are becoming much smarter in relation to their tactics. Most importantly these criminals time their attacks to coincide with global events–namely environmental and political crises–and taking advantage of people at their most vulnerable.

Environmental vulnerability

Environmental vulnerability refers to situations where people are in any way connected or effected by some form of environmental calamity and/or natural disaster. This can include being impacted by bushfires, floods or earthquakes, for example. In these situations, people are focused on rebuilding their life as opposed to cyber threats, resulting in their awareness of warning flags being severely decreased.

An example of this was seen in early 2022 following the destructive floods in New South Wales and Queensland. Many of those impacted received phishing emails purporting to be from their insurers, charities offering help and even from government. Cyber criminals used the floods as a way to entice more people to fall victim to their scams by pretending to offer aid and support. Those targeted were in a vulnerable position and did not notice the warning signs of a scam due to being pre-occupied with the other issues. This illustrates that cyber criminals are becoming more creative in the timing of their attacks and the ways in which they attempt to entice someone to provide their personal information. For example, by pretending to be insurance companies the cyber criminals capitalised on the fact that many people would have been in the process of making insurance claims so, completing one more form providing personal details would not have raised suspicion.

In addition to targeting the victims, cyber criminals also targeted those offering the assistance. Jack Chapman, VP of Threat Intelligence, Egress stated that, "*online donations are often one of the best and fastest ways for people to support a cause, resulting in a quick payday for a cybercriminal running a payment scam that leverages a new or urgent situation*". Not only does this result in much needed donations not reaching those who required the assistance, but it means that people who were not directly impacted by the floods were also targets. Cyber criminals have decided to utilise people's generosity for personal gain knowing that when these events occur, people rush to provide help in any way they can. This reinforces the fact that people who are vulnerable and distracted are more likely to become a victim of cybercrime.

Political vulnerability

Cyber criminals have also been capitalising on times of political unrest. Political vulnerability refers to situations where through conflict, destabilisation of governments or economies, or global pandemics, organisations become more susceptible to cyber-attacks.

In recent years, many different countries have been suspected of carrying out various cyber-attacks on other countries. One of the most destructive attacks was the 'NotPetya' attack in 2017, which caused approximately US$10 billion of damage.

This issue is as relevant today given the ongoing conflict between Russia and Ukraine. Jack Chapman, VP of Threat Intelligence, Egress further advised that, "*most critical infrastructure is delivered through a network of third-party organizations, which increases the pressure on governments and security agencies to ensure they have the necessary protections in place*". As a result of the conflict, there have been concerns that cyber criminals will carry out large scale cyber-attacks on those that align with either Russia or Ukraine. Presently, there have been some reports of cyber-attacks targeting the Ukrainian and Russian government websites. Cyber criminals are very aware of this fact and have used the unrest to their advantage by launching cyber-attacks related to the conflict. There have also been reports of phishing emails impersonating the Ukrainian government and Ukrainian charities seeking financial support. Eric Eekhof, Partner at Korda Mentha also noted that, "*there have been phone calls with Western officials in which a Ukrainian official was impersonated, trying to convince the Western official not to help Ukrainian refugees*".

Similar to the environmental vulnerability, political vulnerability operates in such a way that warning signs are missed. People and organisations are concerned with the events unfolding overseas and are rushing to provide support. Unfortunately, despite good intentions, the cyber criminals are one step ahead and are intercepting these good intentions for their own benefit.

Furthermore, there are some nuanced challenges for insurers and governments caused by government sponsored cyber-attacks. The main issue faced is whether this type of cyber-attack is included in the definition of 'acts of war' in commercial insurance policies.

This issue arose in the New Jersey Superior Court on 13 January 2022. A multinational pharmaceutical company sued its insurer following its claim for coverage of the damage caused by the 'NotPetya' attack being denied on the basis of the exclusion clause citing acts of war. It was held that the insurer could not deny a claim through a reliance on the war exclusion clause in this context as the language used made it clear it was in relation to armed conflict. As a result, the multinational pharmaceutical company was entitled to coverage for $1.4 billion from the cyber-attack.

The key takeaway from this case is that insurers and underwriters need to be mindful of what is and isn't covered in the wording of polices. If insurers wish to ensure that government-sponsored cyber-attacks are not covered, then the exclusion clause wording needs to be updated to reflect the risk that is included and also what is excluded. Clear and unambiguous wording is the key. Insurers should also keep in mind that the burden of proof to rely on an exclusion falls on the insurer; it's not always possible to prove the relationship between cyber criminals and their government sponsor.

How can an organisation limit its vulnerability?

While there is no way to stop these attacks at the source, there are many things that can be done to limit vulnerability to these threats.

First, it is crucial to remain informed about the current trends in cyber-attacks, including how the threat is evolving. Constantly updating devices/systems, improving remote access security, using multifactor authentication and performing regular backups will assist an organisation to continue trading without delay in an event of a cyber-attack.

Further, all individuals and companies should have an incident response plan, which is activated in the event of a cyber-attack. The response plan is vital as it ensures organisations and/or individuals are responding to the attack effectively and promptly to recover data/systems. The plan must be tested and reviewed regularly to ensure efficiency. Along with a response plan, Bec Smith, Director Digital Forensics & Incident Response at Slipstream Cyber Security noted that organisations should be forensic ready and have a business continuity plan. Forensic readiness includes increasing "*the ability to investigate an incident effectively and efficiently through the preservation of evidence, including but not limited to increased log retention and verbosity*".

In relation to a business continuity plan, this is *"built from a formal risk assessment methodology, with well-articulated information security objectives, following a business impact assessment (BIA). A BIA will articulate the means by which systems are recovered, in what order and how quickly"*. In addition, having the appropriate insurance cover will also assist in managing and mitigating the risk that may arise from a cyber-attack.

Second, in times of unrest it is important to remember to slow down and ensure that every time sensitive information is being provided, the person providing the information ensures there are no warning signs.

This includes:

checking email addresses

checking web page URLs

not providing sensitive data over the phone without verifying the caller's identity, and

being cognisant of when something doesn't seem legitimate.

Whenever there is a suspicion that something may not be correct, the best thing to do is take a moment and come back to the decision on whether to provide the data when the situation is not as pressured. Mr Eekhof of Korda Mentha notes that "*this can partially be covered by having the right business processes in place. An example is the four-eyes principle used in financial institutions*".

Finally, never underestimate the importance of training to prevent cyber-attacks. Organisations should prioritise staff attending cybersecurity training to reduce the chances of employees falling victim to cyber-attacks. There should be frequent reviews of the training and policies to ensure that what is being provided remains adequate and also to determine any weak spots that may require improvements.

Prevention is better than cure

Cybersecurity is of the same importance as locking your door at home every night. Criminals are getting smarter at finding new ways to break in despite the continuous innovations in locks.

Cyber criminals operate in the same way. It is important to ensure that an organisation's online 'locks' are up to date and plans are in place to mitigate any issues caused by human error, specifically distractions and vulnerability. Cyber risk is continuously evolving at a high pace. Accordingly, the key takeaway is that prevention is better than cure; it is also cheaper. Given the inevitability of these instances occurring, it is crucial that there are proper plans and procedures in place to appropriately manage the response and mitigate any damage.

THE CHANGING FACE OF THE LEGISLATIVE LANDSCAPE

Author: Partner Jehan Mata
Acknowledgment: Georgie Aidonopoulos

Since 2020 Australia, along with the rest of the world, has experienced an unprecedented shift toward digital reliance and use. Whether through the proliferation of social media applications like TikTok or Meta, remote working or the introduction of tracking apps related to COVID-19, it is unsurprising that cyber-attacks are on the rise.

With the digital space now forming such an integral part of our everyday lives, the Australian Government has undertaken a broad review of Australia's privacy and security legislation, including the *Privacy Amendment (Public Health Contact Information) Act 2020* (the **Act**), the Ransomware *Payments Bill 2021* (No. 2) (the **Ransomware Bill**) and the *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021* (the **Privacy Bill**).

The *Privacy Amendment (Public Health Contact Information) Act* 2020

On 26 April 2020, the Australian Government launched the COVIDSafe app. The COVIDSafe app was an Australian first and was intended to provide a new tool for state and territory health authorities to undertake contact tracing for people exposed to COVID-19.

While each state and territory health authority entered into bilateral agreements regarding the collection, use and disclosure of the COVIDSafe app data, these agreements were enhanced by the Act.

On 14 May 2020, Parliament passed the Act to support the COVIDSafe app and ensure the protection of user privacy.

The Act enshrined the original determination made by the Minister for Health, which contained provisions that:

- ensured the data was only used to support contact tracing efforts
- outlined limited additional instances where data could be used
- required consent before data would be uploaded to the National COVIDSafe Data Store (the **Store**)
- prohibited data from the COVIDSafe app being retained overseas
- required all data held in the Store to be deleted at the end of the pandemic
- protected against decryption, and
- provided that no one can be forced to download or use the CovidSafe app.

The Act introduced additional protections including that:

- The Office of the Australian Information Commissioner (**OAIC**) have oversight of the data contained in COVIDSafe app.
- The Privacy Act's Notifiable Data Breaches scheme extends to the data contained in the COVIDSafe app.
- The administrator of the Store is legally obligated to delete any user's registration data upon request.
- Individuals are required to delete data if they receive it in error.
- No data is permitted to be collected from users who have deleted the COVIDSafe app.
- The Minister for Health must report on the operation and effectiveness of the COVIDSafe app to the Store every six months.

A breach of these requirements was and remains a criminal offence under the Act. For instance, breaches of ss 94E, 94F, 94G, 94H of the Act can lead to imprisonment for five years, or 300 penalty units, or both. These breaches relate to storing COVIDSafe app data outside of Australia; disclosing COVIDSafe app data to another person outside of Australia; decrypting encrypted COVIDSafe app data and requiring another person to download the COVIDSafe app to a communication device.

Comparison with other countries

Many other countries endeavoured to or did introduce a similar application to that of Australia. These countries include Canada, China, France, Germany, Hong Kong, Italy, Indonesia, Poland, Russia, South Africa, Thailand, The Netherlands, Turkey, The United Arab Emirates, the United Kingdom and the United States of America.

Of the counties that developed and implemented an app only Poland, South Africa and the United Arab Emirates did not enact any specific data protection legislation.

Ransomware Payments Bill 2021 (No. 2)

The *Ransomware Payments Bill* 2021 (No. 2) (the **Ransomware Bill**) is in response to the recent ransomware attacks seen on JBS Foods, Nine Entertainment and the Colonial pipeline in the United States.

The purpose of the Ransomware Bill is to provide a mechanism for reporting ransomware payments to the Australian Cyber Security Centre (**ACSC**). According to the Explanatory Memorandum, the information provided to ACSC will be de-identified and provided to the private sector, shared with law enforcement, and used to inform policy making.

A key aspect of the Ransomware Bill is that it defines a person to have engaged in a ransomware attack if:

- the person accesses or modifies data in a computer, impairs electronic communication or impairs the reliability, security or operation of any data on a computer; and the person is aware their access is unauthorised, and
- the person restricts access by authorised personal or gives an unauthorised person access to data, and
- that the person demands a payment to either end the access, prevent publication, end the restriction on access, prevent damage or destruction.

In the event that a ransomware payment is made, the ACSC requires the following information to be reported:

- the name and contact details of the entity
- the identity of the attacker (or what information is known), and
- a description of the ransomware attack.

Notably, indicators of compromise must also be provided that refers to any technical evidence left by the attacker, which may suggest the attacker's identity or methods.

One core issue contributing to the prevalence of ransomware attacks is that many businesses choose not to share experiences if they do fall victim to an attack. This reticence has resulted in under-reporting of ransomware attacks. Other businesses are likely to fall into the trap of believing that the chances of an attack are low. Therefore, businesses that have not yet experienced a ransomware attack are unaware of the significant consequences that may arise.

In addition to the mandatory reporting in the Ransomware Bill, presently any cybersecurity incident experienced by asset owners and critical infrastructure sectors, which has a significant impact on the availability of the asset, must be reported to the ACSC within 12 hours. If the incident is less serious, it must be reported within 72 hours. This mandatory reporting includes ransomware attacks but also extends to any other cyber incidents that disrupt the availability of essential goods and services.

Through the operation of the mandatory reporting, those that fall victim to ransomware attacks will report the attacks, resulting in other businesses becoming more cognisant of the significant risks.

The Ransomware Bill lapsed on 25 July 2022. In order to rectify this, a new Bill must be introduced to Parliament. The Ransomware Bill was originally introduced into the lower house by the Shadow Minister for Cyber Security, Tim Watts but with the recent change of government in Australia and the Labor Party announcing a dedicated Minister for Cyber Security, it is anticipated that a very similar Bill is likely to be tabled again in the near future.

Comparison with other countries

United States of America

The United States' framework for reporting of ransomware payments is similar to the Ransomware Bill. In March 2022, the *Strengthening American Cybersecurity Act* was unanimously passed, which requires any 'substantial cyber incidents' suffered by critical infrastructure entities and civilian federal agencies to be reported to the Department of Homeland Security's Cybersecurity and Infrastructure Agency (**CISA**) within 72 hours. Further, there is a requirement to notify the CISA of any ransomware payments made within 24 hours. This is similar to what would have been the operation of Australia's Ransomware Bill as seen through the mandatory reporting, which will hopefully continue to address the under reporting of ransomware attacks.

United Kingdom

One similarity between the Ransomware Bill and the UK reporting system is that there is a requirement to notify the Information Commission Office (**ICO**) within 72 hours, or without undue delay, after becoming aware of a breach. However, a report is not required if it is unlikely that the breach will impact on the freedoms and rights of individuals.

The ICO and law enforcement do not encourage any ransomware payment. This is on the basis that ransomware demands are made by criminals and there is no guarantee that once payment is made, access to the systems will be returned. It is not uncommon that cyber criminals ask for an initial sum of money to decrypt the data and a further sum to not publish the data. Furthermore, the UK *General Data Protection Regulation* requires 'appropriate measures' to be taken to restore any data that may have been impacted during a cyber-attack. The ICO has provided that in its opinion a payment of a ransom is not an 'appropriate measure'. To add further complexity, if it is suspected that a ransom may or will be used for terrorism, the *Terrorism Act 2000* [United Kingdom of Great Britain and Northern Ireland] provides that the payor may be prosecuted if the ransom is paid. This may result in a prison sentence between six months to 14 years, a fine or both.

Singapore

Singapore's mandatory reporting was established in the *Personal Data Protection Act 2012* (the **PDPA**). The key difference between Australia's Ransomware Bill and the PDPA is the threshold at which mandatory notification is required. The PDPA provides that notification of a data breach is required if firstly, the data breach will likely result or has resulted in significant harm to those impacted by the breach, or secondly, if the data breach will likely or has impacted 500 or more people. The PDPA includes in the definition of a data breach ransomware attacks. Similar to other countries, notification is required within 72 hours, however, the time begins once the breach is determined to be of a nature that must be reported.

Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021

The ***Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill*** **2021**

The (**Privacy Bill**) was introduced in response to privacy challenges posed by the proliferation of social media and online platforms.

Even though over 17 million Australians use social media, there are no legislative protections regarding the potential misuse of personal information by these platforms. This is particularly troubling in the context of the data harvesting scandal of Facebook and Cambridge Analytica in March 2018.

In response to this, the Australian Government aimed to, introduce at the end of 2022 a binding code of practice for social media and other online platforms that trade in personal information. If passed, enhancements would also be made to enforcement mechanisms and penalty provisions under the *Privacy Act*.

Some of the main measures to be introduced include:

- Obtaining informed consent in the context of collection, use and disclosure of personal information.
- The introduction of a binding Online Privacy Code of Practice (the **Code**), which will be co-developed by the Australian Information Commissioner and industry. Additional protections that must be introduced and included in the Code include specific protections for children and other vulnerable persons and a commitment to take reasonable steps to stop using and disclosing a person's information when consent is withdrawn.

- Increasing the penalties for privacy breaches within the *Privacy Act 1988* (Cth). The increases will include:
  - $532,800 for a natural person and $10,000,000 for a body corporate where a serious and/or repeated interference with privacy has occurred
  - a new infringement notice provision regarding the failure to provide information when required as part of an investigation. The maximum civil penalty will be $13,320 for individuals and a maximum of $66,000 for a body corporate, and
  - creating a new criminal penalty for multiple occurrences of non-compliance with the maximum financial penalty to be increased to $66,600 for a body corporate.
- Clarifying the scope of the Extraterritorial application of the *Privacy Act 1988* (Cth) to note that foreign organisations operating within Australia must meet the obligations under the Act, regardless of whether those foreign organisations collect or hold Australian's information directly from a source in Australia.

While the changes came as welcome news in that they would hold "big tech" companies to a higher privacy standard, some institutions have expressed concerns over the ramifications of the Privacy Bill.

In a submission to the Privacy Bill exposure draft, the Insurance Council of Australia, Australian Banking Association, Australian Finance Industry Association and Financial Services Council all warned that the Privacy Bill could lead to "*complexity, potential conflict of laws and outcomes, and higher administrative costs*".

These concerns were raised in the context of the financial sector already operating in a heavily regulated and legally complex environment; the lack of data provided to explain the expanded scope of the Digital Platforms Inquiry beyond the original terms of reference; and unintended consequences of lack of clarity with key terms such as "end user"; inconsistency between the industry between large and small providers; and the lack of transition period.

As the submission advised the then Coalition Government to think over any proposed changes to the finance sector, it will be interesting to see if any amendments to the Bill are made in the coming months.

With the new Labor Government coming into power, it is questionable whether the Privacy Bill will be carried forward. A major criticism of the then Coalition Governments approach to online safety and privacy reform was that it lacked cohesion and was at times uncoordinated. It appears the Labor Government intends to streamline reforms going forward. A timeline nor any real indication as to what will be proposed, or whether any changes will be made to pre-existing reforms, is yet to be made. We will continue to monitor new developments in this area.

More change to come

Due to the speed at which the cyberspace is evolving and its associated risk, governments globally including in Australia, are playing catch up in order to adequately address legislative weaknesses in the cyber and privacy space. Intended Government reforms are a step in the right direction toward mitigating cyber threats and privacy breaches.

Considering the new Labor Government has already noted a desire to bolster Australia's cybersecurity and privacy, it will be interesting to see whether it keeps the former Coalition Government's proposed bills or whether they scrap them and put forward a more streamlined approach. While the Labor Government is yet to comment on whether it intends to do away with the Privacy Bill, if it were to pass the most notable change would be an increase in penalties already in existence within the *Privacy Act 1988* (Cth) and an enforceable, potentially broad reaching Online Privacy Code of Practice.

OPINION PIECE

OUR TAKE ON *INCHCAPE AUSTRALIA LIMITED V CHUBB INSURANCE AUSTRALIA LIMITED* [2022] FCA 883

Author: Partner Jehan Mata
Acknowledgment: Georgie Aidonopoulos

This opinion piece considers some of the issues arising from the case of *Inchcape Australia Limited v Chubb Insurance Australia Limited* [2022] FCA 883 (the **Decision**). A claim was made by Inchcape (the **Insured**) on a 'Chubb Financial Institutions Electronic and Computer Crime Policy' (the **Policy**) seeking to obtain cover for losses arising out of a ransomware attack. The attackers encrypted the Insured's primary server, deleted primary and offsite back-ups, infected laptops and desktop computers with malicious software and published data on the dark web. The Insured incurred financial losses in attempting to repair and/or restore hardware, software and data.

The market offers different types of policies covering a variety of losses. A standard cyber policy will provide liability protection to a company in the event a cyber-attack is suffered, or in the event of a breach. In contrast, this Policy covered damage of electronic data or software, caused by malicious software entering a company's server. The Decision included a detailed discussion on causation and first-party losses; these topics will be canvased in further articles. This article looks at the commercial implications of this Decision on insurers, brokers and insureds.

The Decision

The Court was required to decide on three core questions, all of which were essentially concerned with which of the losses sustained because of the ransomware attack were recoverable under the Policy. Two of the questions were decided in the insurer's favour, meaning that the Insured was only awarded a 'hollow' victory as only one limb of its claim succeeded. As a result, the bulk of the costs it incurred were deemed to not be recoverable under the Policy.

We understand that an application for leave to appeal has been filed and we will provide updates on the status of the appeal.

Insights

This Decision reinforces the importance of all parties being educated about what their commercial insurance policies cover. The fact that the Insured sought indemnity for losses under the Policy and most of the losses were found to be outside the scope of the Policy highlights that insureds and brokers need to be fully aware of what type of coverage they require and ensure that the policy or suite of policies they buy respond to the risks. Furthermore, brokers and insurers must adequately explain the limitations of each policy with prospective insureds to limit the risk of disputes of this kind arising. Litigated disputes such as this can be reduced through clarity of policy wording to ensure that there are no ambiguities as to what is and is not covered. Although this issue is not new or limited to cyber cover, given the ever-changing cyber landscape and developments in technology, it is particularly challenging to stay abreast of the risks that are emerging and policies' responses to these risks.

Readers may already be aware of the concept of "silent cyber", which refers to instances where a non-cyber policy is drafted so broadly that it covers losses arising from a cyber-breach. Business interruption, errors & omissions and directors and officer's insurance policies have in some cases responded to cyber claims in cases where is was questionable if that was ever the intention of the underwriter. Whilst such silent cyber claims seem to be decreasing in number, they do still happen; this Decision involves a claim being made on a non-traditional cyber policy. The Court determined that a majority of the losses were not recoverable under the Policy, which emphasises the importance for parties to be aware of what risk is covered under specific policies. Had the decision fallen in favour of the insured, this case would present a clear example and warning to insurers of the risks of silent cyber.

A key issue in dispute in the Decision concerned causation and whether the loss was as a result of 'direct financial loss'. If leave is granted to appeal this matter, it will be interesting to see how the appellate court considers the intention and operation of the policy.

We have seen similar situations arise on numerous occasions in relation to phishing attacks as they sit between a cyber-attack and a criminal attack. There is a criminal element to phishing attacks, which raises a similar question as to whether this risk sits under the usual cyber policy or whether it is covered in a crime policy.

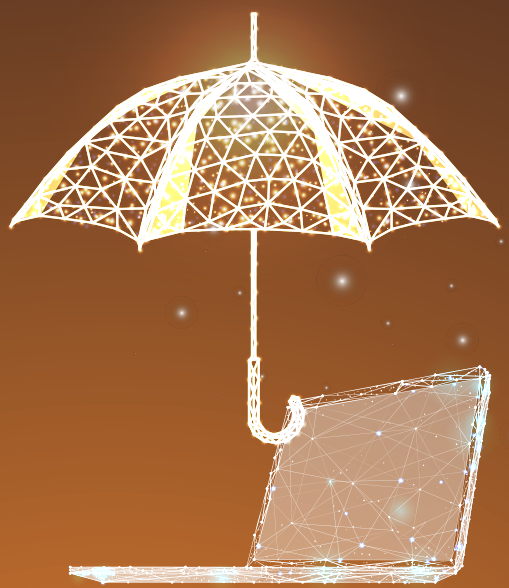
Sparke Helmore Lawyers assist both insurers and insureds to review policy wordings and assess the appropriateness of those wordings. Testing policies' wordings provides assurance to insurers that their wordings meet the intended requirement and provides insureds with the comfort of knowing they are obtaining the cover they require.

If the application for leave to appeal is granted, we will continue to provide updates on this Decision. In the interim, it is essential for parties to be on the front foot about these issues, through education about what policies do and don't cover, and by having a thorough understanding of businesses' needs and the risks – both current and emerging – that they face.

DIY INSURANCE: ARE CAPTIVE INSURERS THE FUTURE OF CYBER INSURANCE?

Author: Partner Jehan Mata
Acknowledgment: Georgie Aidonopoulos

Captive insurers have recently received a lot of attention in the media, but the concept of captive insurance is not a new idea. Captive insurers are companies that effectively insure themselves through setting up an insurance company. This type of arrangement has been around since the 19th century and is very common in most of the Fortune 500 companies. However, in recent years, captive insurers are increasingly being used to cover cyber insurance. There are many benefits and only a few disadvantages in using a captive insurer for cyber insurance coverage.



Positive relationship between captive insurers and cyber insurance

Captive insurers play a vital role in relation to cyber risk.

First, cyber insurance is still relatively new, and some commercial insurers may not have the appetite to adequately deal with this rapidly changing landscape. Therefore, by setting up a captive insurer, a company can ensure that the specific concerns it has regarding its cybersecurity will be addressed in a policy of its own making. The specific needs of a company's cyber insurance policy are largely dependent on the industry, the company and the severity of the threats it is or believes it will be facing. A captive insurer allows for flexibility and ensures that the desired risks are covered. This particular benefit is important as according to Pen Underwriting, "*most insurers are planning to or already sub-limiting, excluding or co-insuring ransomware exposures*". If a company for example is more concerned with ransomware attacks, it can opt for a captive insurer to ensure this risk is adequately covered.

Second, as cyber threats are generally infrequent it is unlikely that a company will experience a major cyber-attack every year. However, when these attacks happen, the harm inflicted can be severe. For this reason, a captive insurance policy can span multiple years to ensure that premiums paid are retained by the captive insurer until a major cyber-attack takes place at which time, the premiums paid will assist in dealing with the situation.

Third, captive insurance can effectively operate as an 'umbrella' over other insurance policies a company has in place. A major cyber-attack will likely impact on several aspects of that company and depending on the severity of the attack, claims may need to be made against other policies such as property or liability insurance. The flexibility of captive insurance allows for the nuanced risks to be addressed so that in the event of a major attack, the company is not facing the issue of being under-insured while also dealing with the consequences of the cyber-attack.

Finally, due to the fact that the company is involved in deciding what is and isn't covered, this increases the likelihood it will have a greater appreciation of the risks. This in turn, may influence company policy and training to ensure that adequate systems are in place to prevent cyber-attacks.

The challenges

Despite the benefits, there is one key challenge that companies face if they decide to utilise a captive insurer. That challenge is the difficulty that may be encountered in convincing all stakeholders to pursue captive insurance. This is because captive insurers are regulated and a company must have sufficient capital to consider this option. Therefore, it may take some time to convince stakeholders that a captive is the best course of action due to the amount of work in setting it up and the continuous investment of time and money in running it.

In order to combat these issues, a company can look towards a reinsurer while they set up a captive insurer to allow time to adequately understand the process and the regulations. Currently, approximately 40% of cyber insurance premiums are being paid to reinsurers, which suggests that it is not uncommon to seek cyber insurance from avenues other than commercial insurers.

Final thoughts

Before a company decides to set up a captive insurance company, there are some very important decisions that need to be made.

It will take significant effort and resources to set up, capitalise and run a captive insurer. An important consideration is which domicile will be used for the captive insurer. A company must also consider the reason behind why it is pursuing a captive insurer and the relevant business needs in selecting a domicile. This is because different domiciles have different regulations, which may make a location more or less attractive depending on the intention of the captive insurer.

Presently, Bermuda is a popular choice with 680 captive insurers domiciled there as of 31 December 2020. Other popular choices include the Cayman Islands, Guernsey, Singapore, Labuan and various states in the United States of America, such as Hawaii. The current trend has been selecting domiciles that have less stringent requirements and which are inherently more flexible—such as Singapore or Labuan—compared to domiciles that have increasingly strict requirements, such as Australia.

Practical considerations also need to be taken into account including the significant time difference from Australia to some of the popular offshore centres such as Bermuda and the availability to adequately staff and operate the captive in the domicile. While it is possible to change domicile, it is useful to select the best option up-front to ensure that unnecessary costs are not being incurred. For large Australian businesses that require flexibility when it comes to wording and are struggling to purchase the right cyber insurance product in the current market, a captive insurer may provide a significant upside.

However, captive insurers reinforce that there are many ways to protect a company against cyber threats and the decision of the type of insurance taken out is very dependent on the company itself.

Sparke Helmore has a leading financial services practice and has experience advising companies on risk management options, including setting up of captive insurers.

SUPPLY CHAINS: YOU ARE ONLY AS STRONG AS YOUR WEAKEST LINK

Author: Partner Jehan Mata
Acknowledgment: Noor Klank

New cyber threats appear every day. In the years leading up to the pandemic, there was a significant increase in cyber-attacks directly against individuals and businesses.

Recently, in 2022, supply chain attacks on organisations (also known as third-party attacks) have become one of the most treacherous known security threats. Additionally, there has been an increase in the volume and sophistication of these attacks in the last year as evidenced by:

- Betanews reported that cyber criminals can breach 93% of an organisation's networks and gain access to its data.
- A recent survey by Anchore found that three out of five companies experienced software supply chain attacks in 2021.
- Only 6% of companies that experienced a third-party attack said the supply chain impact was minor, whilst the remainder of companies were impacted at a moderate to high level.
- Based on NCC Group's research, supply chain attacks increased 51% between July to December of 2021.

Now more than ever, organisations need to implement effective risk management solutions and integrate cybersecurity practices to mitigate the effects of supply chain disruptions.

Supply chain attacks

Times are changing and so is the nature of the supply chain. Companies are constantly looking for new ways to reduce costs and increase profit. One way companies are doing this is by sourcing materials and manufacturing goods all over the world. Around 42% of global exports are sourced in Asia, which makes these exports a prime target for cyber criminals. A supply chain is very rarely linear, rather it is a web that branches in different directions; each entity that is connected to the supply chain has its own web. Entities, suppliers and vendors are all intertwined and can significantly impact one another should a business disruption occur. As a result, a cyber-attack on an Asian facility would create tremendous disruptions to the global supply. Further, entities that export, manufacture or ship through politically unstable countries and areas could also face significant supply chain risks and are highly exposed to disruptions.

So, while companies have been fortifying cybersecurity defences, cyber criminals have been capitalising on one area that remains vulnerable—the supply chain. According to Security Delta (HSD), indirect attacks against weak links in the supply chain accounts for 40% of security breaches.[1] In fact, CrowdStrike 2021 Global Security Attitude Survey (**CrowdStrike Survey**) found that 45% of Australian organisations have experienced a supply chain attack within the last 12 months.[2]

[1] Kelly Bissell, Ryan Lasalle and Paolo Dal Cin, 'Innovate For Cyber Resilience, Lessons from Leaders to Master Cybersecurity Execution', Security Delta (Report, 22 January 2021) 7 <https://securitydelta.nl/media/com_hsd/report/341/document/Accenture-Cybersecurity-Report-2020.pdf>.

[2] Goran Lepan, 'Crowdstrike Global Security Attitude Survey 2021 – The Findings', InfoTrust (Blog Post, 20 January 2022 https://infotrust.com.au/resource-library/crowdstrike-global-security-attitude-survey-2021-the-findings/blog.

Third-party attacks occur when cyber criminals infiltrate an unsecure vendor or supplier system in the chain to gain access to data. The system is then injected with malicious code and/or malware. Once the cyber criminals gain access to a system, they will either move quickly to gain control over the system or will lie dormant for months or even years collecting and exfiltrating data.

Eric Eekhof, Partner at Korda Mentha, provided the following example of a "*marketing firm that receives an overview of all the customer's clients for marketing purposes. In this case the hackers will likely steal the customer's client data…Additionally, the hackers may try to 'jump' to the customer through fake emails sent from the marketing company's email system. The customer's staff may consider these emails more trusted because they come from an existing supplier*".

Accordingly, this will have a flow on effect on the supply chain, which will cause disruptions to any entities connected. Also, these kinds of attacks may have a significant impact on fundamental relationships with partners and suppliers. Mr Eekhof noted that is "*especially in the case that the impacted parties aren't able to recover their costs from insurance policies and try to hold the other party liable to cover their expenses*".

For cyber criminals, third-party attacks are lucrative as they target weak links in the supply chain—those with limited or no cybersecurity—to gain access to a larger organisations without dealing with its sophisticated security control. A single breach can add up to thousands of victims.

Bec Smith, Director Digital Forensics & Incident Response, Slipstream Cyber Security stated that "*by exploiting as-a-service providers and their software, attackers are gaining a powerful foothold*". Fifty per cent of cyber-attacks target a business and those connected to it through a supply chain. Ms Smith highlighted that "*in mid-2022 ransomware groups are still targeting unpatched Microsoft Exchange servers*".

Jack Chapman, VP of Threat Intelligence at Egress stated, "*The most frequent attack method we see is using compromised email accounts to send phishing emails into the customer base. Using compromised supply chain accounts adds legitimacy to a phishing email, often enabling it to avoid detection by perimeter defences and making it appear more convincing to the target.*"

Therefore, it does not appear to matter how vigorous a company's cybersecurity is if a vendor/supplier in the chain does not have an equally sophisticated cybersecurity system in place. So, while companies are taking all the necessary steps to shore up cybersecurity, they must also ensure that other businesses in the supply chain are also adopting similar cybersecurity practices.

A new form of warfare

Over the past years, we have seen global infrastructures come to a standstill as a result of cyber criminals who exploit software supply chain vulnerabilities; the cyber age has introduced the world to a new form of warfare.

Countries have carried out war crimes on critical infrastructure via cyber-attacks leaving countries vulnerable and weak leading current day defence to be trained in cybersecurity. Supply chains have been a primary target for nation state actors, as severe attacks can shut down operations that disable vital commodities. Third-party attacks that gain access to the oil and gas industry, transportation infrastructure, hospitals, electric grid and telecommunications can send an entire country to the stone age and cause tremendous disruptions.

In 2017, Russia compromised Ukrainian accounting software to target its infrastructure by injecting malware (NotPetya), however it quickly spread to other countries. This resulted in US$10 billion in damage and disrupted operations for numerous entities. One of the most recent and well-known supply chain attack was the SolarWinds attack by Russia, which was designed to spy on companies and organisations. The cyber criminals who facilitated the attack capitalised on the multiple supply chain levels. They infiltrated SolarWinds supply chain by injecting a malicious code (a backdoor) into SolarWinds system and infected about 18,000 customers. This allowed the cyber criminals to turn the software into a weapon gaining access to several government systems and organisations all over the world. This attack affected the United States Department of Energy, NASA, the United States Department of Homeland Security, Microsoft and other organisations and agencies. Due to the magnitude of the attack, it cost cyber insurance companies up to US$90 million. Therefore, it is paramount to protect supply chains as they play a significant role in supplying key commodities; if neglected and unprotected, the consequences on the economy could be disastrous.

Third party attacks and cyber insurance

Cyber insurance is an evolving product. A leading international broker has recently reported that the majority of insurers operating in the market are reducing capacity and placing increased attention on pro-active cybersecurity. This would seem to be a consequence of the increases in claims costs, the difficulty pricing cyber risk given its fluctuating nature as well as the increase in ransomware and cyber-attacks making it less enticing for insurers to provide cyber coverage. As a result, cyber policies can change regularly as underwriters have limited information to formulate risk models to determine insurance coverages and premiums. At this stage, cyber insurance policy premiums have increased drastically whilst the coverage for cyber risk has decreased. This has caused a low uptake in cyber policies, especially in SMEs as they are facing economic pressures. In order to make the cyber policies attractive to everyday users, there has to be a level of commerciality i.e. where the coverage of the policy reflects the cost. Currently, the feedback from brokers and underwriters seem to align in that there is a disconnect between the product and its cost.

In relation to third part attacks, many elementary cybersecurity insurances only cover first-party losses. This does not provide coverage for damages stemming from third-party attacks. However, given the increased number of supply chain attacks and disruptions, some insurers are beginning to offer policies that cover third-party liability losses. Such losses include potential loss of profits as well as costs caused by the disruptions to the supply chain. As such, cyber insurance affords various benefits to an entity and its supply chain. That said, cyber insurance is only a defence mechanism and it may not be able to cover reputational and operational business risk, irrespective of the insurance policy purchased the principle stands: better safe than sorry.

Attacks are unavoidable: here's what you can do

Cyber-attacks are inevitable and cannot be prevented. However, steps can be taken to manage and mitigate the flow on effect that may arise from a third-party attack. While it is important to ensure that the appropriate cybersecurity practices and procedures are in place to protect data from unauthorised access, it is just as important to ensure that vendors and other organisations in the supply chain have equally sophisticated cybersecurity systems.

Nearly 50% of organisations don't stipulate security standards when entering into an agreement with suppliers, nor do they regularly monitor or undertake a risk assessment of a supplier's cybersecurity arrangements. This is particularly concerning given the most negative impact occurs from the smallest vendor or supplier in a supply chain. According to the CrowdStrike Survey, the immediate impact of supply chain attacks has resulted in 55% of Australian organisations stating that they have lost trust is key suppliers due to the concerns arising from these attacks.

Jack Chapman, VP of Threat Intelligence at Egress commented that organisations should be "*auditing partners, updating and patching software, and regularly reviewing and reassessing third-party network access. In addition, organisations need to do more to turn the tide against phishing attacks, using training where it is most effective and implementing technology that uses developments like natural language processing and machine learning to determine whether an email is really coming from the expected recipient*".

Another way to ensure that subcontractors take appropriate safety measures is to have contractual provisions, which set the requirements for cybersecurity for vendors entering into an agreement. In addition to mandating cybersecurity, organisations should also include indemnity clauses in its contracts, addressing issues that may arise from a third-party attack. Such contingencies are paramount to manage and minimise disruptions and potential financial blow back from a third-party attack but, also to establish a good relationship with partners and/or suppliers in the chain.

As the attacks are unavoidable, the following key steps (acknowledging Bec Smith, Director Digital Forensics & Incident Response, Slipstream Cyber Security input to these preventative measures) can mitigate the risk of a third-party attack:

Be aware of digital supply chain risk

An organisation must know its risk exposure by cataloguing software and service providers that have remote access to its environment, or whose platforms are critical to business operations. Critical services providers should be asked about its key suppliers.

Wargame your exposure

Often asking hard questions of your supply chain will return an immensely complicated picture and finding a solution can be overwhelming. If that is the case, a next step can be to assume a compromise of these key systems and suppliers, then wargame a response and business continuity arrangements. This process can shine a light on opportunities to build resilience in the organisation. Risks can start to be managed by simply knowing what third-party software and remote access exists, what those systems can touch, and what arrangements the provider has for preventative security and post-breach business continuity can be critical.

Segmentation

Service provider access to a business environment is often necessary, but it's critically important to ensure that access is strictly limited to what is required for the job at hand. The concept of 'least privilege' as it is called in IT security lingo applies as much to software as it does to administrators, and this can be achieved by ensuring software is locked down into compartments that if breached, limit the potential damage. IT management software like Kaseya and SolarWinds have, by-design, powerful high-level privileges hence the importance of restricting access to segments required. Segmentation can require some serious architectural input, but it starts with a next generation firewall and is definitely worth the effort.

Managed Detection and Response

There is no doubt that the most disruptive threats are ransomware and associated data theft extortion, which can occur as a result of supply chain attacks. These threats traverse network perimeters and internally, both on-premises and in the cloud, but ultimately execute on endpoints (servers and user devices). For this reason, the most rapid, practical security gains can be achieved by securing endpoints with Managed Detection and Response (MDR).

A supply chain is only as strong as its weakest link

Cyber criminals are continuously evolving their craft and finding new and lucrative ways to target and capitalise on entities/agencies data. Although these attacks cannot be prevented, there are steps and actions that can be taken to mitigate the impact of a third-party attack including building, maintaining and fostering healthy cybersecurity practices across the supply chain. Don't forget, a supply chain is only as strong as its weakest link.

WHO IS ACCOUNTABLE FOR CYBERSECURITY?

Author: Partner Jehan Mata
Acknowledgment: Georgia Mineo

With much of the global workforce shifting to remote working and many small businesses relying on cloud software, 2021 was one of the most active years on record for cyber-attacks, and one of the costliest; last year alone there was a 60% increase in ransomware attacks against Australian businesses. This increase in attacks is not anticipated to die down any time soon.

Why are small businesses an easy target?

Australian small businesses (**SMEs**) are an easy target for cybercrime. SMEs are *three* times more likely to be targeted by cyber criminals than larger companies (according to Barracuda Networks[1]). This is mostly due to a lack of preparedness, training and awareness and a small fish big pond mentality—"I'm just a small business, why would anyone target me?". Eric Eekhof, Partner at Korda Mentha adds that, "*the lack of budget, combined with the increasing cost of cybersecurity solutions and consulting services, is also adding to this*".

What are the main cyber threats facing small businesses this year?

Despite all that we know or should know about cybersecurity, Australian businesses both large and small are still being caught out by long-standing threats. For instance, the main threats for 2022 have been identified as stock standard issues: phishing and malware attacks, ransomware, weak passwords and employee carelessness.

Even in 2022, with all we know about password security, a run-of-the-mill username and password hack occurred at Deakin University leading to the compromise of nearly 47,000 current and past students contact details. According to Mr Eekhof, this admittedly "*started at one of their suppliers that had stored the credentials of a Deakin staff member. The supplier shouldn't have stored this information and Deakin should have had MFA*".

It is unsurprising therefore that a study by CyberCX found Australian companies to be falling behind international competitors when it comes to protecting the online privacy of customers.[2]

What is Australia doing about this?

The Australian Government has placed cybersecurity and resilience at the forefront of policy reform. Australia's key financial regulators have also identified this as a key area of focus for the coming years and have put businesses and board members on notice to prioritise the enhancement of a cybersecurity posture by treating it as a business function, rather than an issue transferred to an IT department.

While this may be the stance of the government and regulators, the fundamental question remains – what are we *actually* doing to hold businesses accountable for cybersecurity and cyber resilience?

[1] https://www.forbes.com, Small Businesses Are More Frequent Targets of Cyberattacks Than Larger Companies: New Report, Edward Segal, Senior Contributor, 16 May 2022.

[2] John Davidson, 'Which industry protects your privacy best?' Financial Review (online, 6 May 2022) https://www.afr.com/technology/which-industry-protects-your-privacy-best-20220503-p5ai7u

The current accountability framework for businesses

The Office of the Australian Information Commissioner (OAIC)

Australia does not have a private course of action for individuals regarding privacy and data breaches. Traditionally, the OAIC has been tasked with dealing with privacy complaints and data breaches. To date, the ability of the OAIC to enforce penalties that would actively encourage a business to take a proactive approach to strengthen its cybersecurity posture has been limited. While the OAIC can impose financial penalties, so far it has arguably been nominal and unintimidating.

It was welcomed by the OAIC when the Australian Government introduced the draft *Privacy Legislation Amendment (Enhancing Online Privacy and other Measures) Bill 2021* (**Bill**). While it has not yet passed both houses, if it does, it will allow the OAIC to impose higher penalties. The penalties will increase to:

- not more than the greater of $10 million, or
- three times the value of any benefit obtained through the misuse of information, or
- 10% of the entity's annual Australian turnover.

If the Bill is passed, the possibility of receiving one of these penalties will likely encourage a business to reassess its cybersecurity posture This can also be achieved if the OAIC publicly enforces this policy and issues fines to any organisation that breaches its duties.

The Cybersecurity Strategy

Noting the increase in preventable cybersecurity threats and the limited ability of the OAIC to get businesses doing more, it was positive news in 2020 when the Australian Government acknowledged that cybersecurity is a shared responsibility. The Government (at the time) promised to invest $1.67 billion over ten years in cybersecurity, the largest ever financial commitment to cybersecurity.

While the Cybersecurity Strategy focused on a collaborative approach and provided tools to equip businesses with the skills and knowledge needed to strengthen cybersecurity, it was also aimed at introducing an enhanced legal framework that would hold businesses accountable in critical sectors.

The *Security Legislation Amendment (Critical Infrastructure) Act 2021* (Cth) was passed and imposed positive security obligations across twelve sectors including banking and finance; communications; data and cloud; defence; education; research and innovation; energy; food and grocery; health; space; transport and water.

However, the new Labor Government has noted that it will revise the former Coalition Government's 2020 Cybersecurity Strategy. Labor was vocal of its concerns with the 2020 Cybersecurity Strategy, taking issue with its lack of consultation and contemporaneity. Consequently, these revisions will involve greater collaboration, incorporate pandemic developments and factor in the increasing (and ever changing) threat landscape.

The Government wants certainty for the sector and to foster confident responses to threats. There is mention of these revisions to be grounded in sovereign capability, with a focus on the growth and future of the workforce and cybersecurity sector. Labor has shown its commitment to bolstering cybersecurity by giving the topic its own portfolio in the Australian Cabinet, which is a political first. A timeline is yet to be decided. It will likely be a while before we see any revised strategy, noting the government's desire for greater collaboration with the industry.

Regulatory bodies – ASIC

Sticking to its promise of ensuring entities adopt adequate controls and maintain cyber resilience, a landmark test case was brought by ASIC against Australian Financial Services Licensee, RI Advice. ASIC argued that RI Advice should have, but failed to, impose adequate cybersecurity risk management, which resulted in numerous cybersecurity breaches, placing sensitive data at risk.

In an Australian first, this year, the Federal Court found RI Advice in breach of its obligations to have in place adequate risk management systems to manage its cybersecurity risks. While the Court noted that it is "*not possible to reduce cybersecurity risk to zero*", the Court did opine that risks can be reduced to an acceptable level through adequate documentation and controls.

Due to RI Advice's breach, it was ordered to pay $750,000 to ASIC. However, along with other compliance and regulatory steps, the costs would overall be higher than $750,000. The case acts as a warning and timely reminder for entities about strengthening cybersecurity capabilities.

What about accountability for other online platforms like Instagram?

While there has been a governmental and regulatory focus on the business community and implementing measures to hold organisations accountable for cybersecurity, social networking sites have not been forgotten.

A recent ruling by the Full Federal Court in F*acebook Inc v Australian Information Commissioner* [2022] FCAFC 9 confirmed that Facebook Inc was carrying on business in Australia and was collecting and holding personal information in Australia at the time in question and therefore was captured by the operation of the *Privacy Act*. The case stemmed from the Cambridge Analytica scandal and was initially filed by the OAIC in March 2020. With the OAIC obtaining this important ruling and allowing for the proceeding to continue to a hearing of the substantive matter, this decision will provide important guidance on the regulation of social media sites and how they use a user's personal information.

The enforcement action against Facebook has highlighted some of the regulatory difficulties faced in holding social media platform companies accountable for management of data privacy. The *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021* aims to change this. If passed, it will allow the OAIC to register an enforceable online privacy code, which would be binding on social media services and others and could see social media platforms fined up to $10 million for serious privacy breaches.

This degree of power is needed as, to date, social media platforms remain largely unchecked. With the proliferation of sites like TikTok, and an increasing presence of children on these sites, the code would provide much needed privacy and data safety protections particularly for children and would bring Australia in line with other countries.

Accountability of online platforms across the globe

In 2018, the European Union successfully introduced the *General Data Protection Regime* (**GDPR**), which harmonised data privacy laws across all its member countries. It is considered the world's strongest set of data protection rules containing 99 individual articles. Notably, large fines and reputational damages can be imposed for those found in breach of the rules.

While the GDPR is broad in its reach, it successfully managed to place social media platforms on notice, particularly in relation to targeting practices.

Some European countries have enacted complementary legislation to the GDPR, which strengthens the protection of children's data. For instance, the United Kingdom (UK) enacted the *Age Appropriate Design Code* (**the Code**). The Code applies to apps, programs, search engines, social media platforms, amongst others, and applies to both UK and non-UK companies that process the personal data of UK children.

In the United States of America, lawmakers have tried to keep pace with the ever-increasing presence of social media through *The Communications Decency Act* and the *Children's Online Privacy Protection Act*. Currently, no comprehensive social media privacy law exists and nor is there an equivalent to the European Union's GDPR. The only comparable law within the United States is the *California Consumer Privacy Act* (**CCPA**). In addition, Mr Eekhof of Korda Mentha highlighted that the *New York Privacy Act* is similar to the CCPA but, it additionally allows impacted consumers to claim damages.

Saudi Arabia has clear and precise procedures in place regarding the protection of children's data within the *Children and Incompetent's Privacy Protection Policy*. While it falls short of the GDPR by not offering any restrictions for the profiling of minors, it does exceed the GDPR in one area; it clearly mandates that third parties must be assessed and contracted based on the same high level of security as the data collector.

The future of accountability

Cybersecurity is an ever evolving and increasing threat. To date, the Australian Government and regulators have made some progress toward enacting and tabling legislation that will encourage SMEs and large corporations alike to strengthen cybersecurity postures.

In relation to social media, it will be interesting to watch the progression of the legislation to see if it is successful in holding social media platforms to account.

Duncan Cotterill

CURRENT TRENDS OF CYBER RISK IN NEW ZEALAND – THE ROLE OF RISK MANAGEMENT AND INSURANCE

Authors: Partner Tanya Wood
and Senior Associate Peter Fernando

Over the last two years New Zealand insurers have seen a significant increase in the number of notifications and claims for cyber attacks.

What then can New Zealanders do to manage their risk and minimise cyber attacks? In this article we identify what cyber risks Kiwi businesses are currently contending with and look to address how they can manage this risk, and what cyber insurance can do to assist.

Criminal and state-sponsored cyber attacks

The source of our country's main cyber risks are criminal and state sponsored, with phishing and credential harvesting the most reported incident category according to the Government's Computer Emergency Response Team (CERT NZ).

CERT NZ says these types of attacks contribute over 50% of all reported incidents to the organisation. Given the dominance of small and medium enterprises (SMEs) in the New Zealand landscape, there is a high volume of low-level cyber incidents.

Most losses are suffered by organisations and individuals through scams, phishing, and credential harvesting, each of which are perpetrated for financial gain. These include social engineering (such as "romance scams") as well as sophisticated email intrusions resulting in misdirection of funds—especially for property settlements.

Overseas scams and attack targets

For businesses in the corporate space, New Zealand follows global trends with ransomware being at the forefront of loss causes. These attacks are from varied sources but largely originate offshore.

In light of present geo-political factors (including Asia-Pacific trade route and military tensions, and the Russia–Ukraine war), state-sponsored cyber activity regularly affects New Zealand's nationally significant organisations.

This includes distributed denial-of-service (DDoS) attacks—where an attacker sends a vast amount of traffic to a server, stopping people from accessing a digital service—on New Zealand's stock exchange, several banks, power companies, state-owned enterprises, and telecommunications companies.

DDoS attacks have sharply increased over the last five years, with criminal gangs utilising DDoS, or the threat of them, to extort ransoms that are usually payable in cryptocurrency.

Cyber-attacks look more like us and play with our emotions

New Zealand follows the global trend of greater frequency and severity of attacks.

The intricacy of phishing attempts has increased, with New Zealand individuals and businesses being targeted by schemes that are more "localised," including phishing emails written in te reo Maori. There are also convincing campaigns impersonating banks, charities, IT firms, and government agencies.

In the past few years, CERT NZ received reports of email phishing attempts designed to prompt a strong emotional response, including most-recently fake relief efforts for Ukraine.

Due to pandemic restrictions, many businesses were not equipped or adequately secure when forced into remote working. This provided a significant opportunity to exploit deficiencies and weakness, and has played a significant role in the increased number of cyber attacks over the last two years.

Protecting your business

With all of these types of attacks, a robust IT system is crucial. However, we are seeing most cyber incidents are opportunities exploiting individuals in a business. Therefore it is key to have regular training and processes in place to identify when a breach has occurred, and know how to respond to that breach.

CERT NZ have recently issued a helpful incident management guideline. The key recommendations by CERT NZ centre around risk assessment and ensuring that business have an incident plan in the event of cyber attack. The role that insurance can play, in order to mitigate the practical and economic risk of a cyber attack, is essential in this current environment.

Cyber insurance in NZ generally provides cover for network security breaches, privacy breach and confidentiality breaches. The cover will often pay for the cost of first response professionals to investigate and retore the network, along with loss of income and the payment of fines and penalties from privacy breaches.

Looking forward we see changes likely to the insurance cover available for extortions or ransoms. The traditional approach is to exclude cover for terrorism. However, with the growing increase in state sponsored cyber terrorism, we would expect the definition of a cyber-attack to change what is included. State sponsored cyber attacks are likely to be included within the exclusions of cover moving forward.

The uptake of cyber cover in NZ is still well behind Australia. This is perhaps not surprising given our mandatory privacy reporting obligations have only been in place since the inception of the Privacy Act in 2020. Subject to changes in underwriting criteria for some businesses, we expect that there will be a growing uptake of cyber cover over the next year.

New baseline set for cyber insurance

Over the past 24 months, the local cyber insurance market has undertaken a significant adjustment. A new baseline has been set with regards to premium, deductible levels, coverage availability, capacity, and underwriting rigor.

There are now certain baseline criteria to obtain cyber cover, which include:

- The use of Anti Malware software;
- Backing up data regularly;
- the use of Multi Factor Authentication and VPN (when working remotely);
- Ensuring that software updates are actioned regularly; and
- Updating default credentials.

While obtaining the necessary underwriting criteria to obtain cover can be challenging due to the unique requirements of each insurer, there is still good cover, and capacity for cover in the NZ market.. Some businesses may need to make some changes to how they operate, in order to obtain cyber insurance cover, and businesses may see an increase in the premium they pay for cover.

Cyber insurance risks

Ensuring you understand your cyber risk, and planning for a cyber attack is now essential for NZ businesses. It is not a matter of it, but when a cyber attack will occur. Not only will this planning assist in the prevention of an attack, but it will also demonstrate to insurers that you are a risk they are prepared to underwrite.

Why Sparke Helmore?

Sparke Helmore's national cyber practice, led by Partners Jehan Mata, Mark Doepel and Dalvin Chien, offers comprehensive cyber expertise across both individual and company risk. Our extensive experience includes advising on privacy notifications and notifiable data breach issues, cyber policy drafting, acting as coverage and monitoring counsel, and managing recovery efforts, including asset tracing and subrogated claims.

Our clients benefit from our experience across the full spectrum of cyber breach matters. We manage claims efficiently and provide strategic advice on legal and regulatory exposures. We engage in risk mitigation with both insureds and insurers on "Lifecycle Issues" (through training, incident response triage, third-party contract reviews, and coordinating service provider support during times of breach). In addition to providing advice, we help educate our clients on emerging cyber trends and topics. Our team has presented extensively on cyber insurance and contributed significantly to thought leadership in this space.

As a full-service firm, Sparke Helmore leverages the expertise of our technology law and advisory specialists along with our panel of third-party vendors to support our clients on their end-to-end cyber lifecycle needs. We have a thorough knowledge of the cyber solutions, platforms and providers in the market and can provide insights into innovative cyber risk solutions. Given the potential for a cyber claim to have wide-reaching international regulatory exposure, we can assist with any offshore cyber-related matters, leveraging our affiliated members through our Global Insurance Law Connect network.

Contact details

To find out about the ways that we can help you, please contact a member of our team:

Jehan Mata
Partner
t: +61 3 9291 2374 | e: jehan.mata@sparke.com.au

Mark Doepel
Partner
t: +61 2 9260 2445 | e: mark.doepel@sparke.com.au

Dalvin Chien
Partner
t: +61 2 9260 2537 | e: dalvin.chien@sparke.com.au

sparke HELMORE LAWYERS

www.sparke.com.au

adelaide | brisbane | canberra | darwin | melbourne | newcastle | perth | sydney | upper hunter