sparke HELMORE LAWYERS

Cyber **Rewind**

MAIN TAKEAWAYS FOR 2023

DEC 2023 ISSUE 2

Jehan Mata

Partner
Sparke Helmore

With another year coming to an end, cyber continues to feature at the top of the 'hot topic' list. As a result, cyber risk and cyber insurance remain at the forefront of many industries' minds heading into 2024.

In addition to our half-yearly report on cyber trends, in this update are some of the key trends from 2023 and our take on what the industry should keep an eye on in 2024.

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

We would like to acknowledge the contribution of Georgie Aidonopoulos and Georgia Mineo in the preparation of this update.

INCREASE IN SEVERITY & EXPENSE OF CYBER ATTACKS

According to the 2023 Cost of a Data Breach report prepared by IBM Security, an increase in the recovery and expense of a cyber-attack was reported. The headline from the IBM report saw

- 2.3% in the average total cost of a data breach to USD 4.45 million, and
- the lifecycle of a cyber incident increased to approximately 277 days from detection to containment.

Healthcare under attack

The Australian healthcare sector continues to be the most targeted industry by cybercriminals. According to the Office of the Australian Information Commissioner **(OAIC)**, in the second half of 2022, the sector reported the highest number of notified breaches in Australia, with almost 20% of all incidents. We expect a continuing upward trend in 2024. Some of the high-profile breaches this year include:

- The Crown Princess Mary Cancer Centre in Westmead Hospital. Cybercriminal group Medusa claimed to have stolen thousands of files, holding the facility for ransom.
- Royal Women's Hospital cyberattack of October 2023. 200 patient records were accessed due to a staff member's personal email being compromised.

Our research suggests that the healthcare sector is a consistent target for three reasons:

1. Private patient information is worth a lot of money to attackers.
2. The sector is most likely to pay ransom, due to the higher risks posed to national security and the health risks posed to patients if the sector is unable to undertake day-to-day activities and the concerns with reputational damage.
3. Politically motivated threat actors are aware of the chaos a crashed healthcare system can cause.
4. Smaller healthcare organisations will continue to be at greater risk, given their less complex and up-to-date cybersecurity solutions and their appearance as an easy back-door gateway to larger companies.

Generative AI in insurance

AI will also continue to be a hot topic in 2024. The use of AI is expected to grow with speculation that more insurers will adopt generative AI in the next few years. AI will likely be deployed in the near future for customer service assistance, contract drafting and auditing. It will be interesting to see whether more insurers begin to use AI to achieve maximum efficiency in handling claims and assessing risk.

We are also keen to see how insurers factor in AI risks into policies in 2024. Given the popular sales during the festive season, it will be worth noting if insurers factor in scams using AI tools that impersonate businesses, like ChatGPT, which is said to be a rising trend. We are also curious to see if insurers take the same stance as banks in not compensating for damage caused by these scams.

Cloud servers at risk

Eighty-two per cent of breaches involved data stored in the cloud. Due to this, there is a need in the market for companies to protect their data in cloud servers much more than in previous years. In light of the current data breach class actions, protecting personal information and data is even more critical than before.

Class action status

In an Australian first, data breach class actions have been filed in the Federal Court of Australia **(FCA)** and the Victorian Supreme Court on behalf of the victims of the Optus and Medibank breaches.

- Optus – A consumer class action has been filed in the FCA.
- Medibank – Initially, two consumer class actions were filed in the FCA, which have since been consolidated. Two shareholder class action were also filed in the Supreme Court of Victoria; however, these have also been consolidated. (There are also the OAIC investigation in respect of this breach.)

The class actions are in addition to the regulatory investigations and associated proceedings discussed below.

Given the class actions are in the early stage, there is no indication of when these actions will finalise. Plaintiff firms are interested in commencing a similar action against Latitude Financial in the new year.

As a right to privacy is yet to be codified within Australian law, these actions centre on breaches of contract, confidence, continuous disclosure obligations and engaging in misleading and deceptive conduct. We believe the key takeaways from the above proceedings will be:

- If breach is established, given there is only guidance on cyber defences and management rather than an actual legal mandate.
- What are the relevant threshold/legal tests.
- How loss is quantified, particularly non-economic loss for things like emotional distress, mental anguish, and trauma.
- How courts deal with investigative material obtained by businesses in the wake of a data breach.

We have already seen this come to the forefront in the Optus class action, where a claim for privilege over a report Optus obtained from Deloitte following the breach, was rejected. It is important to note that it was rejected as it was not requested/obtained for the dominant purpose of obtaining legal advice or for use in litigation/regulatory proceedings.

Uptick in regulatory investigations

Although the class actions are certainly a point of interest, we urge insurers, businesses, and brokers to not overlook the response of the OAIC, Australian Securities and Investment Commission **(ASIC)** and the Australian Prudential and Regulation Authority **(APRA)** to cyber breaches. We expect to see a continuing uptick in regulatory investigations and prosecutions in 2024.

We have noticed an increased interest from the OAIC to commence proceedings against businesses embroiled in cyber breaches. Proceedings to keep an eye on in 2024 include the recent action against Australian Clinical Labs Limited **(ACL)**. In February 2022, ACL's Medlab Pathology business was hacked, affecting 223,000 individuals medical data. The OAIC was first notified of the incident in July 2022, with its investigation into the ACL's privacy practices commencing in December 2022. Now that the OAIC has finalised its investigation, it has commenced proceedings in the Federal Court. This is significant, as it is only the second time that the OAIC has done this, despite having the power to do so since 2014. It will also be interesting to see the outcome of the OAIC investigation into the Optus breach, given $5.5 million in funding has been allocated to assist this process.

Similar to our take on the class actions, the outcomes of the above proceeding (and potential Optus proceeding) will provide guidance as to how the OAIC will quantify and assess awards for loss and damages. This will be particularly relevant to businesses, insurers, and brokers from a policy, coverage and reserving standpoint considering:

- the maximum penalties for serious or repeated privacy breaches were increased late last year from $2.22million to whichever is the greater of: $50 million; three times the value of any benefit obtained through the misuse of information; or 30% of a company's adjusted turnover in the relevant period.

ASIC

Earlier this year ASIC Chair, Joe Longo, stated that ASIC is looking for an appropriate vehicle to prosecute **individuals** for failing to take appropriate steps to ensure companies have appropriate cyber arrangements in place.

APRA

APRA announced earlier this year that following a review of Medibank's cyber incident in October 2022, that it would impose an increase in Medibank's capital adequacy requirement of $250 million. APRA Member Suzanne Smith said that this action was to ensure that Medibank expedites its remediation program. APRA has also warned that it will take further action against entities to ensure gaps and weaknesses in cybersecurity control measures are addressed.

Insurers, businesses, and brokers will need to stay on top of the legal and regulatory landscape in 2024.

OAIC COMPENSATION AWARDS

The Administrative Appeals Tribunal recently handed down a decision regarding a cyber breach, which addressed the assessment of quantum. The following table provided as part of the decision gives cyber practitioners important guidance when assessing quantum from a data breach.

Category	Description	Quantum
0	Any individual who has not provided a submission and/or evidence that substantiates loss or damage resulting from the data breach.	$0
1	Minor loss or damage resulting from the data breach (for example, general anxiousness, fear, anger, stress, worry concern or embarrassment).	$500 - $4,000
2	Moderate loss or damage resulting from the data breach (for example, moderate anxiousness, stress, fear, pain and suffering, distress and/or humiliation), which has caused minor physiological symptoms, such as some loss of sleep or headaches.	$4,001 - $8,000
3	Major loss or damage resulting from the data breach (for example, major or prolonged anxiousness, stress, fear, pain and suffering, distress, humiliation, loss of sleep, and/or headaches) which has caused psychological and/or physiological harm and has resulted in a consultation with a health practitioner.	$8,001 - $12,000
4	Significant loss or damage resulting from the data breach (for example, the development or exacerbation of a diagnosed psychological or other medical condition), which has resulted in a prescribed course of treatment from a medical practitioner.	$12,001 - $20,000
5	Extreme loss or damage resulting from the data breach.	> $20,000

CYBERSECURITY LEGISLATION

Statutory tort of privacy

As discussed in our previous article, the Attorney General has recommended introducing a statutory tort of privacy. Since that update, the Attorney General has "agreed in-principle" that the tort should be introduced based on the model recommended by the Australian Law Reform Commission **(ALRC)** in its Report 123:

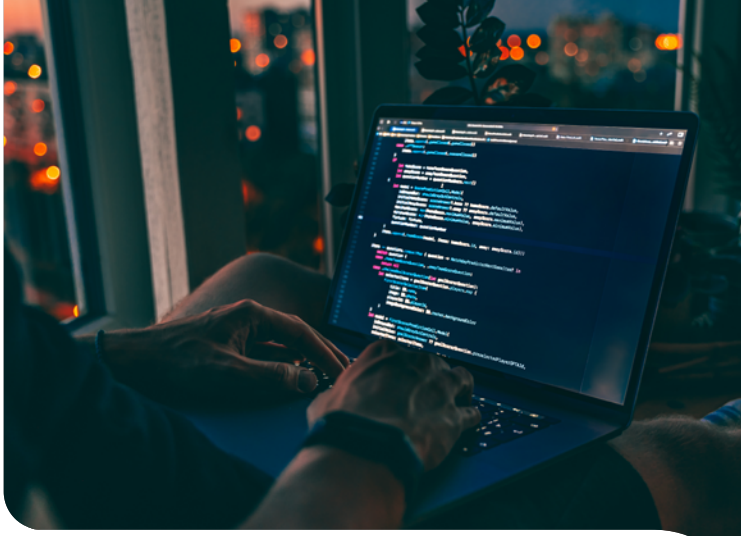
- the tort should be enacted in a Commonwealth Act
- the plaintiff must prove that their privacy was invaded through *(a)* intrusion upon seclusion, or *(b)* misuse of private information
- it must be proved that a person in the position of the plaintiff would have had a reasonable expectation of privacy in all of the circumstances
- it should be confirmed to intentional or reckless invasions of privacy, not negligence
- the invasion of privacy was "serious"
- the plaintiff should not be required to prove actual damage
- the court must be satisfied that the public interest in privacy outweighs any countervailing public interest, and
- the public interest in privacy outweighs any countervailing public interest.

The ALRC recommended various defences to a finding of a breach of privacy, including:

- lawful authority
- incidental to defence of persons or property
- consent
- necessity
- absolute privilege
- publication of public documents, and
- fair report of proceedings of public concerns.

The ALRC has also recommended a variety of remedies that should be available to a plaintiff if a breach of privacy is found, including:

- Damages (including emotional distress)
- Exemplary damages (exceptional circumstances)
- Account of profits
- Injunctions
- Delivery and destruction or removal of material
- Apologies and correction
- Declarations



Although the consensus within the legal industry is that the ALRC recommendations will be adopted, the Australian Government has said it will only enact the new tort once further engagement with regulated entities and a comprehensive impact analysis has taken place. As a tort of privacy is an Australian first, all avenues need to be exhausted to ensure that the right balance between freedom of publication and an individual's right to privacy is struck before it is codified.

Mandatory Notification of Data Breach Scheme

As part of the amendments to the *Privacy and Personal Information Protection* Act 1998 **(the PIPP Act)**, the Federal Government has introduced a new Mandatory Notification of Data Breach Scheme, which came into effect on 28 November 2023. The amendments will require public sector agencies bound by the PPIP Act to notify the Privacy Commissioner and affected individuals of data breaches. All agencies are expected (within reason) to contain, assess and reduce the damage of a breach within 30 days of becoming aware of it.

Security Legislation Amendment (Critical Infrastructure Protection) Act 2022

Following the Optus hack of 2022, Home Affairs Minister Clare O'Neil announced on 13 November 2023 that telecommunications will be classed as "critical infrastructure" for the first time once new laws are introduced. This will require company boards to comply with strict rules and sign off on new or updated cyber risk management programs yearly or face hefty penalties.

Cyber Incident Review Board

The Department of Home Affairs announced this month that a new Cyber Incident Review Board **(the Board)** will be established. The Board will be responsible for running investigations into major cyber-attacks in an effort to gain a better insight in how to defend Australia from threat actors. The investigations will be classed as "no-fault", meaning they are not designed to prosecute or name a breached organisation; the investigations will focus on data collection and understanding Australia's cyber defences. The aim of investigations will be to share with the broader community and public, by way of published reports, the lessons and insights gained from reviewing breaches to facilitate improving Australia's cyber resilience.

As these highlights show, 2024 is shaping up to be a critical year for data breach investigations, class actions, and legislative reforms in Australia.

THINGS TO WATCH IN 2024

With every passing year, we see an increase in cyber-attacks and the repetition of the phrases cyber resilience and cyber preparedness. Based on the above, below are our hot tips for the industry in 2024.

- Be cyber savvy. A balance between security *and* resilience is vital.
- Stay on top of judicial decisions and legislative changes. These will convey the:
  - courts' expectations of cyber preparedness and resilience
  - thresholds and financial penalties for cyber breaches, and
  - will act as a current guide for insurers on the appropriate wording of definitions and insurable risks clauses.
- Health sector beware. All security reports suggest the sector is a major target. Security hygiene, attack preparation, security tools and adaptive technologies need to be considered in 2024, particularly for small practices.
- Consider your personal security. Given some attacks occurred due to the use of personal email addresses, individuals should look into the benefits of personal cyber insurance.
- Consider any personal risk cyber. There may be an increasing market for personal cyber insurance.
- Factor in investigation costs to your budget. Increased regulatory scrutiny = increased investigation costs.
- Keep a look-out for the use of AI and any reported risks.
- Back to basics – The minefield of applying privilege on investigation reports is not novel and retaining lawyers at the earliest possible time post incident and having an incident response plan can help navigate those risks.
- Consider professional indemnity risks, particularly for brokers. As brokers are the intermediary between insurers and insureds, it is important they receive proper training and understand cyber policies, coverage amounts, and the impact of exclusions.

Aside from the above, in 2024, we will be interested to see the uptake and usage of cyber war exclusions, which have received particular interest in the London market since mid-year. Given the current political market and the increase influence of hostile state actors, we believe this is a section of the market to keep an eye on, particularly how the exclusion and definitions are phrased.

sparke HELMORE LAWYERS

About Sparke Helmore

Sparke Helmore's national cyber practice, led by Partner Jehan Mata offers comprehensive cyber expertise across both individual and company risk.

We can help you manage cyber claims with expertise in coverage, regulatory and incident management. We can also advise you on risk management strategies and trends in the market, indemnity/claims issues regarding commercial contracts and projects, and help draft and review cyber policies for compliance. Beyond coverage, we assist with recovery action.

We distinguish ourselves from other players in the market as specialists in regulatory issues and other associated privacy issues and class actions. These are key areas of focus as Australia moves toward the development of the tort of privacy, following recent cyber-attacks on large Australian organisations. We can help you forecast and manage emerging risks (including technology, AI and the tort of privacy) and we consider future trends which will impact underwriters writing risk in Australia.

In addition to providing advice, we help educate our clients on emerging cyber trends and topics.

Leveraging our national footprint and global reach via our London practice and membership of the Global Insurance Law Connect (GILC) - an independent network of insurance specialist law firms, we combine national expertise with extensive experience advising international insurers and insureds.