SIMPSON GRIERSON

Cyber risks - be prepared

April 2025

Contents

Introduction

In recent years, our clients have increasingly called on us to manage the legal risks arising from cyber-incidents, whether the result of human error or attacks by malicious actors. In parallel, requests for advice on how to proactively minimise those risks before an incident arises are also on the rise.

These observations reflect the reality of doing business in New Zealand in 2025, where organisations hold more data than ever before while facing the triple threat of unprecedented levels of cyber-crime, regulatory oversight and litigation risk.

It follows that the time is right to publish this, our first report on navigating the legal implications of cyber risks in New Zealand. In the pages that follow we highlight the current key areas of legal exposure and look ahead to those on the horizon. You will also find practical guidance to manage these risks in a rapidly changing legal landscape. We hope you find the insights useful.

Jania Baigent, Partner
Head of Cybersecurity & Data Disputes

01 Key facts & forecasts: a snapshot

44%
increase in cyber-attacks worldwide in 2024.[1]

$1.1 billion USD reported in 2023

Cyber-crime on the rise

The New Zealand National Cyber Security Centre received reports of $6.8 million in direct financial losses from cyber-crime in Q4 2024, up 24% from Q3.[2] Recent estimates forecast that the losses caused by cyber-crime globally will reach **$10.5 trillion by 2025**,[3] due in part to advances in generative AI and the additional scope it offers for scams and frauds.

Ransom payments: a new norm

Ransomware continues to be a cyber-crime hot-spot, with crypto-currency **ransom payments of US$1.1 billion** reportedly paid in 2023,[4] reflecting that organisations are increasingly willing to pay hackers to mitigate the effects of data theft. The global cyber insurance market is reported to have almost tripled in size over the past five years and ransomware is forecast to continue to be one of the largest risk and loss drivers for insurers.

Cyber in the courts & director exposure

In the short term, we expect to see continued use of **urgent interim injunctions** to prevent use and publication of lost or stolen data. The Australian trend towards **class actions** by organisations and individuals affected by data breaches is likely to reach New Zealand's shores. We also expect boards to be under scrutiny, with off shore cases and commentators focusing on **director exposure** for failures to deal adequately with cyber risks at a governance level.

Prioritise privacy

We expect complaints to the Office of the **Privacy Commissioner** regarding **data breaches** to increase, and the Commissioner to continue to use the limited tools available to deter and sanction cyber-related privacy breaches. It remains to be seen whether Parliament will heed the Commissioner's repeated calls for greater enforcement powers.

Law-makers try to keep pace

New Zealand has yet to introduce a specific cyber-security statute but New Zealand businesses operating across the Tasman need to be aware that the **Australian Cyber Security Legislative Package 2024** has recently passed into law. Amongst other things, the legislation makes it mandatory for large organisations to **disclose ransomware payments**.

1. *The State of Cyber Security 2025, Check Point Software Technologies Ltd.*
2. *CERT: Quarter Four Cyber Security Insights 2024: https://www.cert.govt.nz/insights-and-research/quarterly-report/quarter-four-cyber-security-insights-2024/*
3. *https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/*
4. *https://www.theguardian.com/technology/2024/feb/07/ransomware-gangs-staged-comeback-last-year-says-crypto-research-firm*

02 Context: the state of the nation

There is no doubt that cyber-crime is a rapidly increasing threat to all organisations. New Zealand's National Cyber Security Centre (**NCSC**) reports that it handled 1,358 cyber incidents in Q4 2024, with 100 of those affecting nationally significant organisations or with potential to cause national harm.

Kordia's New Zealand **Business Cyber Security Report 2025** records that 59% of businesses surveyed experienced a cyber incident in the past 12 months, with 43% of attacks and incidents involving email phishing and others arising from a variety of circumstances including through unsecured websites/applications, cloud misconfiguration or vulnerability and AI breaches.

Cyber threat trends

Continuing and emerging threats for 2025 include the following:

- **Identity theft:** Microsoft reports that there are over 600 million cyber-attacks a day worldwide.[5] In New Zealand, the DIA estimates that identity crimes may cost the New Zealand economy in excess of $200 million each year.[6]

- **Artificial intelligence:** The increasing accessibility and proliferation of AI technologies lowers the barrier for malicious cyber activity at a scale and level of sophistication previously outside the capabilities of cyber-criminals, including phishing, vishing and deepfakes.[7]

- **Ransomware:** Kordia reports that "data theft paired with ransomware has become the norm". This trend seems set to continue with the proliferation of ransomware-as-a-service business models (where cyber-criminals sell their ransomware code to others) creating opportunities for smaller players to enter the cyber-extortion market.

- **State-sponsored attacks:** Global tensions and warfare are leading to an increase in state-sponsored attacks worldwide. In New Zealand, the NCSC has reported an increase in Russian-state linked malicious cyber-activity, noting it is increasingly difficult to disassociate or attribute state and criminal cyber activity.[8]

Costs to business

Needless to say, the costs and consequences of cyber-attacks are biting. According to the NCSC, **losses of $44 million** were reportedly caused by cyber-incidents in New Zealand over the last two years.[9] Global figures dwarf this amount. The 2024 CrowdStrike incident is estimated to cost Fortune 500 companies alone more than $5 billion in direct losses.[10]

The consequences go beyond direct financial costs. A wide variety of impacts often follow cyber incidents, including supply chain and business disruption, ransom payments, reputational damage, compromised IP and commercially sensitive data, and employee resignations.

5. https://news.microsoft.com/en-cee/2024/11/29/microsoft-digital-defense-report-600-million-cyberattacks-per-day-around-the-globe/
6. https://www.dia.govt.nz/Identity---What-is-identity-theft
7. https://www.ncsc.govt.nz/resources/ncsc-annual-cyber-threat-reports/2024-web
8. https://www.ncsc.govt.nz/resources/ncsc-annual-cyber-threat-reports/2024-web
9. https://cyble.com/blog/ncsc-reports-6-8m-losses-in-q4-2024/
10. https://fortune.com/2024/08/03/crowdstrike-outage-fortune-500-companies-5-4-billion-damages-uninsured-losses/

03 Director liability for cyber incidents: a new frontier

Discussions with our clients make it clear that directors are increasingly aware that good governance in the digital age requires an understanding and active management of cyber-security risks.

This awareness is well-merited. While New Zealand directors have yet to face legal action in relation to cyber-incidents, developments overseas highlight that personal liability is a real and emerging risk for boards in this country.

Key areas of potential exposure include the following:

- **Breach of statutory duties:** Companies Act duties to act in the best interests of the company and to exercise reasonable care, diligence and skill are broad enough to encompass acts (and omissions) relating to cyber-attacks and data breaches.

  The risks arise throughout the life-cycle of a cyber-incident, from failure to take adequate steps to prevent a breach (for example through a lack of appropriate cyber-security policies or ignoring known risks or deficiencies) to mishandling the response to an attack (such as, failing to take adequate measures to contain or mitigate the effects of the breach).

- **Fair Trading Act:** Directors may be personally liable under the Fair Trading Act for misleading representations about the security of systems or how their organisation manages and stores sensitive or personal information (see our discussion of the US SolarWinds case in the international developments section). This risk particularly arises in small companies (where the director is the company's alter-ego) or where the director has taken personal responsibility for the accuracy of the representations.

- **Breaches of continuous disclosure obligations:** The Financial Market Authority's recent successful enforcement action against directors and a CFO in the CBL litigation highlights that senior executives and directors can have accessory liability for breaches of continuous disclosure obligations. This could potentially extend to a failure to disclose known cyber-security deficiencies (the basis of the Australian shareholder class action against Medibank, discussed on page 7).

"It is clear that where directors have the requisite level of knowledge of, and involvement in, a breach by the company they face a real risk of significant personal liability. Managing cyber risk is a critical issue for many boards, particularly as directors increasingly find themselves in the crosshairs of regulators, shareholders, and consumers alike. The stakes are certainly high." g forward".

Nina Blomfield, Head of Litigation, Simpson Grierson

04 Director liability: international developments

Governance exposure related to cyber-attacks is of increasing concern to boards. We look at international developments below.

The **USA** leads the way in cyber-related litigation against directors, who have faced several high-profile shareholder **derivative actions** for breach of fiduciary duty following cyber-attacks. These include claims against the directors of SolarWinds for failing to monitor cyber-security risks and legal action against the directors of Marriott for failing to carry out proper due diligence on a cyber-security system, continuing to operate it and failing to report a data breach in a timely manner.

"If things go wrong, ASIC will be looking for the right case where company directors and boards failed to take reasonable steps, or make reasonable investments proportionate to the risks that their business poses."[14]

Joe Longo, ASIC Chair

While those claims were unsuccessful,[11] in 2019, former directors of Yahoo settled breach of duty claims for **US$29 million** following data leaks affecting all three billion Yahoo users. The alleged breaches included failures to follow industry standards, respond to data breaches or provide and train adequate staff.

The risks extend beyond derivative actions. In 2022, Uber's former chief security officer was **convicted for obstructing justice** by attempting to cover-up that the company had been hacked. More recently, an **SEC action** against SolarWinds' CISO was upheld while other charges were dismissed. The Court held the **CISO liable for misleading statements** about the company's cyber-security controls in the Security Statement on SolarWinds' website, finding that he had approved the statement despite knowing of inaccuracies in it.

In **Australia**, ASIC has made it clear to directors that failing to give sufficient priority to cyber-security and cyber-resilience exposes them to action for breach of the duty to exercise powers with due care and diligence.[12] It is reported to have begun legal action against unnamed directors in 2024.[13]

11. *The unsuccessful claims were based on Delaware's Caremark doctrine which imposes personal liability for corporate traumas caused by legal violations on directors who knowingly or utterly breach those duties. This is a high threshold: https://corpgov.law.harvard.edu/2025/03/18/caremark-liability-for-materially-misleading-cybersecurity-disclosures-solar-winds-reconsidered/*
12. *Reported by the Australian Institute of Directors: https://www.aicd.com.au/risk-management/framework/cyber-security/regulators-warn-directors-to-step-up-on-cyber-threats.html#:~:text=%E2%80%9CASIC%20expects%20directors%20to%20ensure,to%20meet%20your%20regulatory%20obligations.%E2%80%9D*
13. *https://www.afr.com/technology/asic-pursues-board-directors-over-cyber-breaches-20240911-p5k9t0*
14. *https://www.afr.com/technology/asic-pursues-board-directors-over-cyber-breaches-20240911-p5k9t0*

05 Data breaches in the courts: class actions

While a class action arising out of a cyber-attack or data-breach has yet to be filed in New Zealand, developments in Australia indicate that this is an area to watch. Particularly given the steady rise in class action filings in New Zealand in recent years, and the increased presence of litigation funding (see our class actions guide here).

In Australia, class actions are underway or in contemplation in relation to three major cyber-attacks (against telecommunications provider Optus, financial services provider Latitude Financial and health insurer Medibank (see our case study here). The result of these actions will have a significant impact on the likelihood of New Zealand class actions in this space.

Common features of the Australian class actions which we expect to see replicated here include:

- They tend to be brought on behalf of **consumers** or **shareholders**
- They include claims that the defendants failed to take appropriate steps to **protect the data** affected, including because of **inadequate cyber-security** measures
- The legal grounds for the claims include **breach of contract**, breach of **consumer law**, breach of **confidence**, breach of a **duty of care**, breach of **privacy legislation** and, in the case of shareholder claims, breach of **continuous disclosure obligations**
- Difficult issues of **loss and causation** arise
- They can, and often do, run alongside **regulatory investigations** and **prosecutions**.

Looking further offshore, class actions following data breaches are rife in the US. According to a recent report by a US law firm, the top 10 class action settlements in the data breach space totalled US$593.2 million in 2024.[15]

A possible chill on class actions: difficulties in proving loss

Difficulties in establishing financial loss is a common feature in consumer class actions relating to data breaches. In most cases, the affected organisation will already have compensated affected individuals for direct costs such as replacing documents (Optus is reported to have put aside AU$140 million for these and other costs resulting from the hack on its system). Beyond those direct costs it is usually difficult for plaintiffs to identify additional direct costs because it is not clear what, if any, use the stolen information has been put to.

It remains to be seen how willing the Australian courts are to order general damages for emotional harm and distress in the Optus and Medibank consumer actions. In June 2024, the Federal Court struck out a claim by an individual affected by the Latitude Financial data breach because he had failed to establish loss or damage. In dismissing the claim, the judge noted that the applicant's case "rises no higher than the allegation that personal data relating to him has been made available to third parties who may engage in fraud or identity theft."

Not all mass data breaches will result in harm meriting substantial damages of that size but where classes are large, even small individual awards quickly add up into six figures and beyond.

15. https://www.duanemorris.com/pressreleases/duane_morris_llp_publishes_its_data_breach_class_action_review_2025_0225.html

Medibank: a class action case study

Australian health insurer Medibank suffered a cyber-attack in 2022, after credentials saved by an IT contractor to an internet browser on his personal device were stolen by Russian criminals who used them to access Medibank's network. It is alleged that at the time of the attack, Medibank had been informed by external experts that its failure to require multi-factor authentication (MFA) for access to its network was a "critical" defect and that it had failed to take steps to address this.

Sensitive data of up to 9.7 million customers was affected and the hackers leaked some of it onto the dark web after Medibank failed to pay the ransom demanded.

Medibank is facing multiple lawsuits including two consumer class actions, a shareholder class action and a civil penalty action by the Australian privacy regulator for breach of its obligations under the Australian Privacy Act.

The **consumer class actions** allege that Medibank breached:

- **customer contracts** by failing to comply with various terms including that it would ensure all information was stored securely and only for as long as required;
- **its duties of care and confidence to customers** by failing to implement appropriate cyber-security measures, including MFA; and
- **the Australian Consumer Law** (equivalent to New Zealand's Fair Trading Act) by making misleading misrepresentations regarding the standards and sufficiency of its cyber controls.

The **shareholder class action** claims that Medibank breached its **continuous disclosure obligations.** It alleges that, prior to the data breach, Medibank was aware of deficiencies in its non-compliance with information security standards but failed to disclose this information to the ASX in breach of its obligations under the Corporations Act. The shareholders claim that this failure caused the market price of Medibank shares to be inflated so that investors purchased those shares at a higher price than they would otherwise have paid.

06 The interim injunction: the first line of legal defence

Court orders can mitigate loss where there is a risk that stolen data will be published.

Urgent injunctive court orders prohibiting use and disclosure of hacked data have become an important legal tool engaged in many of New Zealand's major cyber breaches. While the hackers themselves are unlikely to abide by these orders, they deter use and publication of the stolen data by law-abiding citizens, including mainstream media outlets.

These orders, which apply to "all unknown respondents" (ie the public at large) are becoming increasingly common in New Zealand. The Office of the Privacy Commissioner has described them as a "valuable tool in the data breach toolkit" which prove the "value of accessing the courts quickly to protect the public's interests".

Acting swiftly to obtain urgent orders is an effective and relatively low-cost risk-mitigation strategy for organisations affected by cyber-attacks.

Mercury IT case study

In December 2022, the managed service provider, Mercury IT, suffered a ransomware attack which affected the data it stored for numerous clients, including the Ministry of Justice and Health New Zealand - Te Whatu Ora. The stolen data included coronial files which the cyber criminals threatened to disclose on the dark web.

Given the sensitivity of the data, Simpson Grierson, acting for the Ministry and Health New Zealand, applied for urgent orders preventing all "unknown" defendants from accessing or performing any operations on the stolen data set. The Court granted the orders, noting that the use or disclosure of the data would cause harm to those affected and would likely also generate increased interest on the part of the media and the public who would be encouraged to search for and review the data for their own purposes.

The Office of the Privacy Commissioner supported the application.

"Reaching out to courts can help prevent further harm by making it clear to everyone, that no one should breach the confidences that apply to that compromised data."

Office of the Privacy Commissioner

07 Regulator action: OPC

Businesses need to know about the enforcement powers of the NZ regulator most engaged in investigating and taking action in relation to cyber-breaches, the Office of the Privacy Commissioner (OPC). These include:

- **Fines for non-notification:** Under the Privacy Act, any organisation that suffers a privacy breach that is likely to cause anyone serious harm must notify the OPC and any affected persons as soon as practicable. Failure to do so exposes the organisation to a fine of up to **$10,000.** Further detail is available in our **Privacy Breach Checklist** here.

- **Investigations:** The OPC may investigate privacy breaches and issue **compliance notices** requiring organisations to take action to address breaches of the Privacy Act. The OPC can take enforcement action where a breach identified in a notice is not remedied, including obtaining an order under which a failure to comply may result in a fine of up to $10,000. The OPC has been conducting a joint investigation with its Australian counterpart, the Office of the Australian Information Commissioner (**OAIC**), into the Latitude Financial data breach that affected up to 14 million customer records. Recently the OPC has begun investigating the mishandling of data within New Zealand's public sector following the outcome of public inquiries. See our article on these inquiries and **practical tips** on compliance with the Privacy Act here.

- **Naming policy:** The OPC uses the power to publicly name organisations that fail to comply with the Act as a low-cost deterrent and enforcement tool. While it does not have an immediate financial cost, being "named and shamed" can result in reputational and related damage (see our article here).

The OPC has repeatedly called for greater enforcement powers but to date no reforms in this space are on the legislative books in NZ. Meanwhile, the OPC looks with envy across the Tasman at the tools available to the OAIC (see our article here).

New Zealand businesses with Australian arms should be aware of the recent amendments to the **Australian Privacy Act**. Amongst other things, these increase the OAIC's powers of enforcement, introducing new tiers of civil penalties and enable it to issue infringement and compliance notices.

The OAIC can fine organisations up to the greater of $50 million, three times the benefit accrued through the misuse of the data, or 30% of the organisation's turnover.

08 Regulator action in the financial sector: FMA & RBNZ

Following a thematic review of cyber-resilience in New Zealand financial services by the Financial Markets Authority (FMA), an increasing number of cyber-security obligations apply to organisations under the FMA's remit, including licensed financial advisers, certain market licence holders and financial institutions licensed under the Conduct of Financial Institutions regime.

Broadly, the obligations require the organisations to ensure the operational resilience of critical technology systems and to promptly notify the FMA of any event that materially impacts that resilience. Penalties for breaches include fines of up to $5 million. Additional obligations apply to operators of designated Financial Market Infrastructures[16] which must have cyber-resilience strategies and frameworks that are comprehensive, adequate and credible and must ensure that their compliance with them is assessed by an external auditor every two years.

Since 2024, entities regulated by the Reserve Bank of New Zealand (**RBNZ**) have also been required to notify RBNZ of any "material cyber incidents" within 72 hours. These are information security incidents that materially affect, or have the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries, or other customers.

While New Zealand has yet to see any enforcement action for breach of financial cyber-resilience obligations, the Australian regulator, Australian Securities and Investments Commission (ASIC), has actively pursued licensees in breach of their duties:

- **AU$1.25 million penalty against Lanterne Fund Services:** In 2024, the Federal Court found that wholesale licensee Lanterne had failed to comply with its duties to have adequate technological resources to provide the licensed financial services and to have adequate risk management systems. Relevant factors included that Lanterne did not have an adequate IT infrastructure, IT resources plan, security management plan, IT back-up protocol or disaster recovery plan, and maintained its records using a paper filing system until September 2020.

- **Compliance orders against RI Advice:** In 2022, the Federal Court held that licensee RI Advice breached its duty to have adequate risk management systems, following nine cyber-attacks affecting its authorised representative network. These included the hacking of an email account, which resulted in a client transferring $50,000 in response to a fraudulent email and a ransomware attack affecting the personal information of 220 clients. RI Advice was ordered to appoint an external cyber-security expert and pay costs of $750,000 to ASIC.

- **Legal action against FIIG Securities:** In March 2025, ASIC announced legal action against licensee FIIG Securities for "systemic and prolonged cyber-security failures" that it alleges enabled the theft of confidential data potentially affecting 18,000 clients.

16. *FMIs provide channels through which payments, securities, derivatives or other financial transactions are cleared, settled or recorded*

09 Managing the risks: practical guidance for directors

Managing the risk day-to-day

There is no one size fits all approach to managing cyber risk at board level, but international case law and regulatory guidance contains some common themes:

Be accountable:

Directors are ultimately accountable for the cyber-security of a company. It must be a regular agenda item and, where possible, boards should include a member with appropriate IT experience and expertise (for example, the CTO). That said, cyber-security is an issue for the board as a whole and all members need to understand and be able to engage with the risks.

Risk management framework:

Data governance is increasingly a priority for boards. Risks should be identified, documented and regularly reviewed, as should risk management measures. An obvious area of risk, which should be routinely addressed, is the retention of unnecessary data (see our article here).

Tech-up:

Have adequate cyber-security measures in place, regularly test them and update them as necessary. Consider engaging external experts to audit those measures.

If you see a problem, fix it:

Organisations need to act swiftly to address any cyber-security deficiencies or weaknesses identified. A failure to do so will expose the organisation, and potentially its directors, to liability if that weakness is subsequently exploited.

Create a culture:

According to a recent Mimecast report, 95% of data breaches are caused by human error and human risk has surpassed technology gaps as the biggest cyber-security challenge for organisations around the globe.[17] Regular cyber-security training at all levels is essential.

Look at the supply chain:

Where third parties deal with data on behalf of an organisation, risks can be managed by doing appropriate due diligence on contractors and ensuring that contracts with those parties contain appropriate warranties and indemnities. See our article here.

Be prepared for the worst:

Organisations should have in place emergency response plans, so that they are in a position to act swiftly to mitigate the damage resulting from a cyber breach. We discuss plans further on page 14.

Take a view on ransoms:

Whether or not to pay a cyber-ransom is a key decision for a board and one that it should consider conceptually prior to an attack happening (see our comments on page 16).

Practice the response:

We recommend that boards run regular table-top **cyber-breach simulations** involving all members of the response team. These are useful exercises enabling organisations to work through their response plans and identify weaknesses before being put to the test in a real-life scenario.

Consider insurance:

Most commercial insurance policies will specifically exclude losses (including business interruption) arising from cyber-crime or data breaches unless specific cyber insurance is taken out. The global cyber insurance market has reached a size of US$14 billion in 2023 and is estimated to increase to around US$29 billion by 2027.[18]

17. https://www.mimecast.com/resources/ebooks/state-of-human-risk-2025/
18. https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2024.html

Dealing with a cyber-breach

As noted above, organisations should prepare for the worst and have in place a **cyber-breach response** plan to mitigate damage and preserve business continuity. Plans should include the following steps:

Contain and assess the breach:

Work out what has happened and what immediate steps can be taken to contain the damage. Plans should include remediation and recovery measures to the extent it is possible to formulate these in advance.

Assemble the response team:

The response plan should name key internal stakeholders and assign them responsibilities. External legal and IT support should be identified, in case needed. Organisations may also wish to engage external communications advisers in case the breach attracts negative publicity or reputational damage.

Involve the insurer:

Organisations with cyber-insurance should report the incident promptly. Failure to do so may affect cover.

Consider an injunction:

Urgent injunctive relief may be available to prevent access, disclosure or use of affected data.[19]

Look at your contracts:

Contracts should be checked to determine whether any liability might arise to counter-parties and/or whether they need to be notified.

Have a tight and focused comms strategy

See our case study **Careful with the comms: avoid the blame game** on page 18.

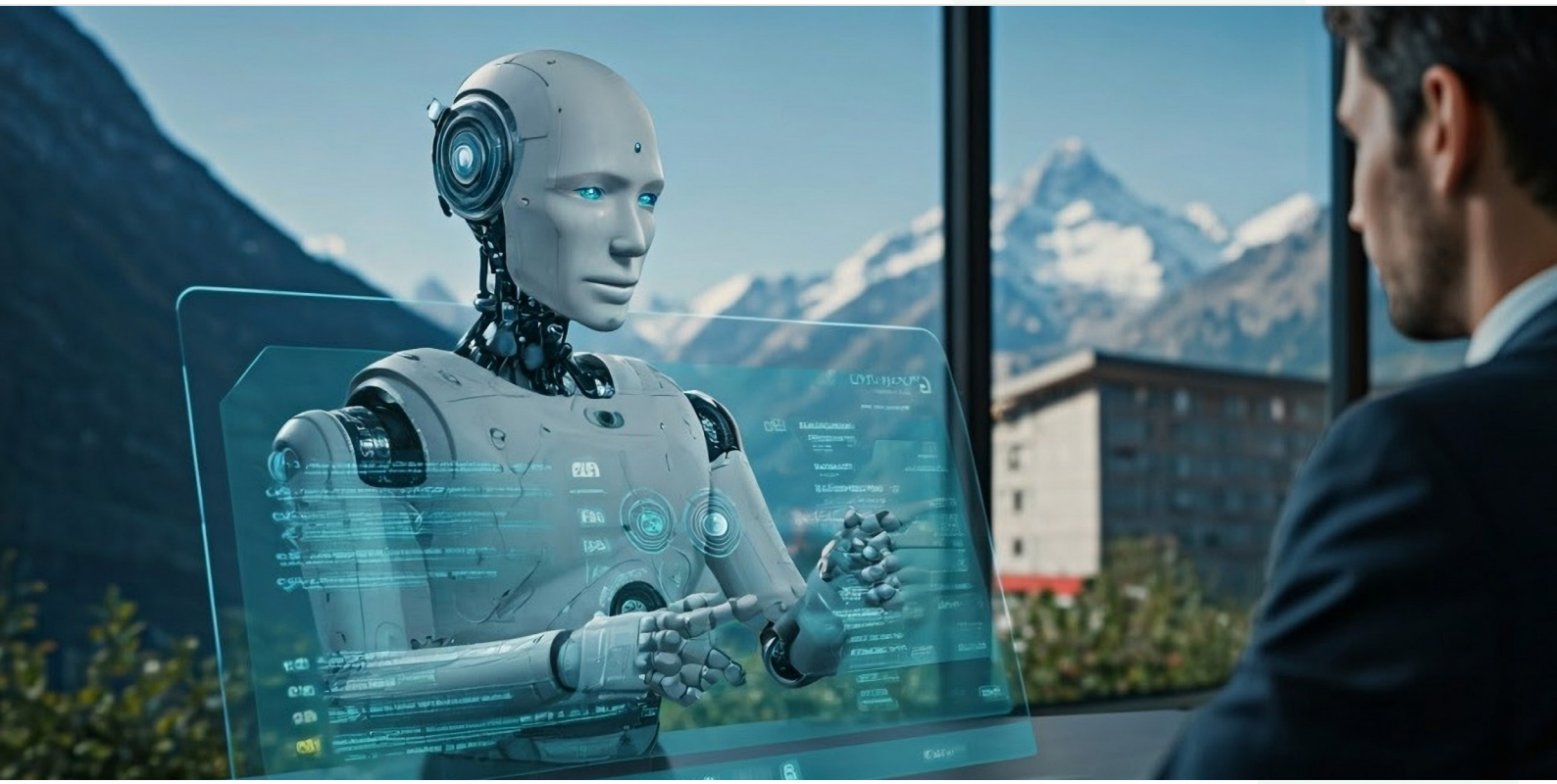
19. *Our firm has obtained a number of such injunctions, including in relation to the recent Mercury IT hack. The Privacy Commissioner called the injunction in that case "a valuable tool in the data breach toolkit": Office of the Privacy Commissioner | Injunctions - a valuable tool in data breach toolkit*

Notify the right agencies:

If the cyber-incident results in a privacy breach that is likely to cause "serious harm", notify the **OPC** and affected individuals (see here). Organisations in the financial sector should consider whether they have an obligation to notify the **FMA** or the **RBNZ** (see page 10) and whether the breach gives rise to **continuous disclosure obligations.** Government agencies are required to report all cyber-security incidents to the **NCSC.**

But don't notify prematurely:

Careful consideration needs to be given to the timing of notifications, within the applicable limits. Going too soon risks presenting regulators and affected third parties with a confused or panicked account of events and an unclear mitigation strategy. This can lead to distress to affected individuals, reputational damage and unnecessary legal exposure.



Ransoms: to pay or not to pay?

In New Zealand, paying a cyber-ransom will be illegal if it breaches sanctions regimes. Breaches carry criminal penalties of up to seven years in prison and fines of $100,000 for individuals, while organisations face fines of up to $1 million.

Even where sanctions are not an issue, the New Zealand Government recommends not paying ransoms, noting that it does not guarantee the return of data and encourages criminal activity. Government agencies do not pay cyber-ransoms.[20]

Despite this advice, **ransomware payments are a reality in New Zealand.** A recent report indicates that of NZ businesses which had experienced a ransomware attack within the past two years **44% paid a ransom,** despite 89% having issued public pledges not to.[21]

There are a number of other indicators that ransom payments are becoming mainstream:

- In 2024, the Australian Institute of Company Directors published a "decision-tree" and detailed guidance to assist boards deciding whether to pay when facing a ransomware attack, recognising that the decision is complex and involves a range of considerations.[22]
- The **Australian Cyber Security Act 2024** has introduced a requirement that Australian businesses with annual turnover exceeding AU$3 million **must report any ransomware payments** to the Department of Home Affairs within 72 hours. At this stage, there is no indication that a similar requirement will be introduced into New Zealand law.
- Insurers are increasingly offering **ransomware cover** as part of cyber-insurance policies, extending to payment of extortion monies and certain costs (for example forensic experts). Global insurance giant Marsh reported that the median extortion payment by its clients increased from US$335,000 in 2022 to US$6.5 million in 2025.

Businesses holding cyber insurance which are contemplating paying a ransom should ensure they consult their insurer and experts before making a payment. Professional ransomware negotiators often handle communications with the hackers and, through experience in similar scenarios, may have a view on the "trustworthiness" of the cyber criminals (some of whom trade on their reputation to keep their "business" afloat) that will feed into the decision as to whether to pay. Regardless of the insurance position, victims of extortion attempts should be cautious of going it alone. Legal advisors and cyber-recovery experts should be high on the contact list if a ransom is demanded.

20. *https://www.dpmc.govt.nz/our-programmes/national-security/cyber-security-strategy/cyber-ransom-advice*
21. *https://www.nzherald.co.nz/business/companies/telecommunications/businesses-pay-cyber-ransoms-on-the-sly/D4NEAMXK6ZHW5PBBT4UE67MLOY/*
22. *Governing Through a Cyber Crisis - Cyber Incident Response and Recovery for Australian Directors*

Ransomware-as-a-Service (RaaS) models will become even more competitive in dark web markets, partly because AI can drive or enhance them. AI will encourage a high degree of automation in hacking processes and lead to a strong individualisation of attacks - with tailored phishing or email extortion that can be easily translated into multiple languages in high quality by AI and thus scaled in many regions simultaneously.

Munich Re | Cyber Insurance Risks and Trends 2024

Careful with the comms: avoid the blame game

Where litigation or regulatory action follows a cyber-attack, communications about the incident, including the unhelpful ones, may have to be produced to the plaintiffs or the regulator, unless they are subject to legal privilege.

For this reason, it is important that in the immediate aftermath of a cyber-breach, careful communication protocols should be put in place. Circulation lists should be kept tight and documents, including emails, text messages and meeting minutes should avoid jumping to conclusions, speculating about the cause of the incident or casually apportioning blame.

Careful consideration is also required further down the track, including where documents are created as part of a formal investigation into what went wrong. Whether privilege protects these documents can be a vexed issue and merits the involvement of legal advisers.

The complexity of the privilege position is illustrated by disclosure disputes in two of the large Australian data breach class actions.

- **Optus** appointed Deloitte to conduct an independent review of its large data breach in 2022 and Deloitte provided its report to the company's General Counsel and external lawyers. Optus refused to disclose it in discovery to the class action plaintiffs, arguing it was privileged because it had been prepared for the dominant purpose of litigation. The court disagreed, finding that while there was a legal purpose to the report, it was also prepared for non-legal purposes. These were recorded in the Board resolution appointing Deloitte as: to identify the root causes of the attack for management purposes; and to review management's policies and processes in relation to cyber-risk.
- **Medibank** was similarly unsuccessful in claiming legal privilege over three Deloitte reports relating to its own cyber-breach. The court found that the reports had been commissioned for multiple purposes, including to update the ASX and assuage market concerns and for public relations, by showing that Medibank was looking to learn from the cyber-incident. Further, if privilege had attached to the reports, Medibank would have waived it to the extent that it referred to certain recommendations in ASX announcements.

Protect your privilege

A key takeaway from the Optus and Medibank decisions is to consider legal privilege at an early stage and build it into your breach strategy.

10 Our cyber team

Jania Baigent
Partner
jania.baigent@simpsongrierson.com
DD +64 9 977 5113 | M +64 21 550 554

Karen Ngan
Partner
karen.ngan@simpsongrierson.com
DD +64 9 977 5080 | M +64 21 648 977

Anita Birkinshaw
Special Counsel
anita.birkinshaw@simpsongrierson.com
DD +64 9 977 5341 | M +64 21 576 735

Michelle Dunlop
Senior Associate
michelle.dunlop@simpsongrierson.com
DD +64 9 977 5325 | M +64 21 302 751

Jonathan Nicolle
Senior Associate
jonathan.nicolle@simpsongrierson.com
DD +64 3 968 4092 | M +64 21 227 3642

Elizabeth Keall-Ross
Senior Associate
elizabeth.keall-ross@simpsongrierson.com
DD +64 9 977 5138 | M +64 21 758 684

Auckland
Level 27, 88 Shortland Street
Private Bag 92518
Auckland 1141
New Zealand
+64 9 358 2222

Wellington
Level 5, 40 Bowen Street
PO Box 2402
Wellington 6140
New Zealand
+64 4 499 4599

Christchurch
Level 1, 151 Cambridge Terrace
West End, PO Box 874
Christchurch 8140
New Zealand
+64 3 365 9914