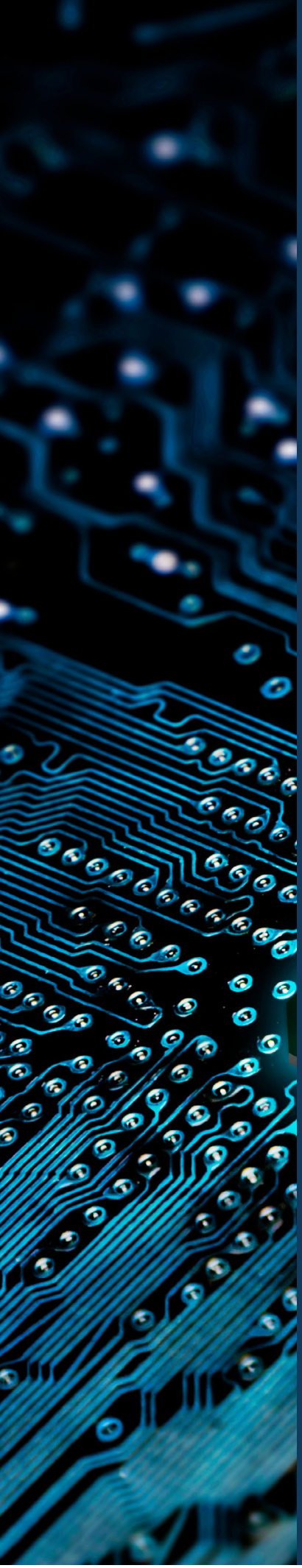
Australian cyber security trends

February 2024

CORRS CHAMBERS WESTGARTH

corrs.com.au

Contents



Foreword

The cyber security landscape in Australia is evolving at a pace.

Aside from the growing number of cyber security incidents, the legal and regulatory environment continues to develop to manage the increased risk. Australian regulators have pointed to increasing responsibility for relevant officers to implement appropriate cyber security safeguards, cyber insurance has developed further and, as widely reported, companies have faced legal action and regulatory investigations in relation to a number of prominent cyber security incidents.

Against this backdrop, we are seeing organisations take a number of operational measures in order to minimise their exposure in the event of a cyber attack. Not only do these measures include necessary increases in security in order to meet the threat of cyber attacks and comply with relevant legislation such as mandatory data breach reporting, they also include:

- reviewing data retention policies;
- assessing the risk of secondary systems such as back-up systems;
- engaging in more detailed dialogue with third party suppliers concerning their cyber security preparedness;
- reviewing cyber security insurances; and
- expanding due diligence enquiries into cyber issues when undertaking major transactions.

In this publication, we highlight some of the key trends in cyber security in Australia to help organisations better understand what kind of cyber incidents are most prevalent in Australia. We unpack key components of organisations' legal and regulatory obligations, and explore Australia's new Cyber Security Strategy, looking at how different regulations intersect for different industries. We also consider how organisations can utilise cyber insurance, what they should be asking of external service providers, and how to embed cyber security into M&A transactions.

Our observations are based on the experience of our cyber security team as well as an assessment of certain publicly available resources.

Philip Catania

Partner and Chair –
Data & AI, TMT Practice Group

+61 3 9672 3333 | +61 419 320 815
philip.catania@corrs.com.au

Executive summary

The 2023-2030 Australian Cyber Security Strategy, released in late 2023, responds to an evolving cyber threat landscape. Core law reforms on new cyber obligations and streamlined reporting obligations are to occur by 2025. Beyond this, the Strategy has not yet proposed any specific timeframes for reforms, and industry consultation will drive the next stage of reforms.

Importantly, the Strategy sends a strong message to Australian organisations: **business cyber resilience is a priority.**

The latest data on cyber security illustrates why:

- During the 2022-23 financial year, over 94,000 cybercrime incidents were reported to law enforcement – an increase of 23% from the previous financial year
- Federal, state and local government sectors reported the highest number of cyber security incidents in the 2022-23 financial year, with professional, scientific and technical services, educational and training and health care and social assistance being the sectors that reported the next highest number of incidents
- According to Sophos' State of Ransomware 2023 research, in 30% of attacks where data was encrypted, data was also exfiltrated
- Historically, ransoms have been paid in 20% of cyber incidents, which has declined over the last few years to around 10-15%, and the Federal Government is considering introducing laws that would make it illegal to pay ransoms demanded by cyber criminals

In the meantime, organisations face an increasingly complex kaleidoscope of regulatory obligations regarding cyber security, including:

- the Privacy Act and the Attorney-General's proposed reforms to it;
- APRA's standards, imposing reporting obligations for financial institutions;
- Security of Critical Infrastructure obligations; and
- the intersection of cyber security and directors' duties.

Many of these regulatory obligations extend to organisations' technology service providers, requiring them to address the issue of the 'cyber adequacy' of the service provider and the consequences if that service provider suffers from a cyber attack.

Cyber security considerations have also become a key focus area in M&A transactions, particularly where the target company holds significant customer data.

Litigation, class action and enforcement risks are increasing too, with an unprecedented number of data breach class actions following a series of high-profile, large-scale Australian data breaches. In parallel, ASIC and the OAIC have signalled increasing focus on regulatory investigations and enforcement action following cyber incidents.

Demand for cyber insurance has also escalated, and is now a critical component of Australian organisations' cyber risk management strategies. Insurers are closely scrutinising the cyber risks of potential insureds to determine whether to underwrite a particular risk and on what terms.

Five steps to help organisations boost their cyber resilience

1. Understand your current regulatory obligations and existing policies around privacy and data retention.
2. Consider upcoming reforms and how new standards might impact your organisation.
3. Look at existing Australian and international frameworks to establish a 'baseline' of cyber resilience.
4. Carefully consider how your organisation would respond to a cyber attack, looking at cyber insurance and approaches to ransom demands.
5. Embed cyber resilience into everything your organisation does – including major transactions and agreements with service providers.

Australia's Cyber Security Strategy

Australia's recently released Cyber Security Strategy seeks to strike a balance between fostering close collaboration between government and industry, and cracking down on businesses that are not 'cyber-ready'.

On 22 November 2023, the Minister for Home Affairs and Cyber Security, the Hon. Clare O'Neil MP, released the 2023-2030 Australian Cyber Security Strategy (**Strategy**).

Responding to an evolving cyber-threat landscape, the message of the Strategy is clear: **business cyber resilience is a priority**. While certain legislative reforms have been proposed, including to the *Security of Critical Infrastructure Act 2018* (Cth) (**SOCI Act**), no economy-wide cyber laws have been proposed at this stage. Further industry consultation will be conducted prior to the introduction of substantive reforms. In the meantime, organisations should ensure they comply with their existing regulatory obligations.

Some key takeaways from the Strategy for directors, general counsel and C-suite personnel include:

- **The proposal to legislate a mandatory no-fault, no-liability ransomware reporting obligation,** which will require businesses to report ransomware incidents. However, the Strategy does not go as far as prohibiting ransomware payments (although the Minister for Home Affairs and Cyber Security has noted that such a prohibition is 'inevitable').
- **No specific cyber security related director's duty has been proposed.** However, the Strategy does focus on increasing cyber discussions in the boardroom and proposes providing further guidance to organisations and directors in relation to cyber security considerations. Additionally, the Federal Government will publish an overview of corporate obligations for critical infrastructure owners and operators that are regulated by the **SOCI** Act.
- Additionally for critical infrastructure entities, **the Strategy seeks to close an unintended regulatory gap,** whereby the SOCI Act does not cover business-critical data storage systems of critical infrastructure owners and operators. Additionally, it would extend the SOCI Act to cover the telecommunications sector.
- The Strategy acknowledges that organisations are subject to a disparate patchwork of sector specific data retention obligations, which may increase unnecessary data retention in Australia. To reduce this risk, **the Strategy proposes a review of Australia's data retention requirements.**
- The Strategy proposes the Government be provided a **broad last resort 'all-hazards consequence management' power.** Details of the precise scope of the proposed power are not provided. However, it appears that it would empower the Government to be able to order specific actions to manage consequences of nationally significant cyber incidents.

The Strategy will be rolled out across three stages or 'horizons' between 2023 and 2030. These are:

- **Horizon 1:** The strengthening of foundations from 2023-2025.
- **Horizon 2:** Scaling of cyber maturity across the whole economy from 2026-2028.
- **Horizon 3:** Becoming a world leader in cyber security by 2030.

Core law reforms on new cyber obligations and streamlined reporting obligations are to occur between 2023 and 2025. Beyond this, the Strategy has not proposed any specific timeframes for reforms, and the Government will conduct in-depth industry consultation prior to introducing any further reforms.

Alongside the Strategy, the Government has developed the Cyber Security Strategy Action Plan (**Action Plan**). It supplements the Strategy and details the key initiatives that will commence over the next two years. The Government will release an updated Action Plan every two years.

The future of Australia's cyber security strategy is of great significance as the nation navigates an increasingly complex digital landscape. As the reliance on digital infrastructure continues to expand across sectors, a comprehensive and proactive cyber security strategy is crucial to safeguarding national interests, critical infrastructure and personal data.

As Australia aims to be at the forefront of cyber security reform and strives to achieve cyber resilience, the Government's next steps will be critical.

View our recent article for more information on Australia's 2023-2030 Cyber Security Strategy.

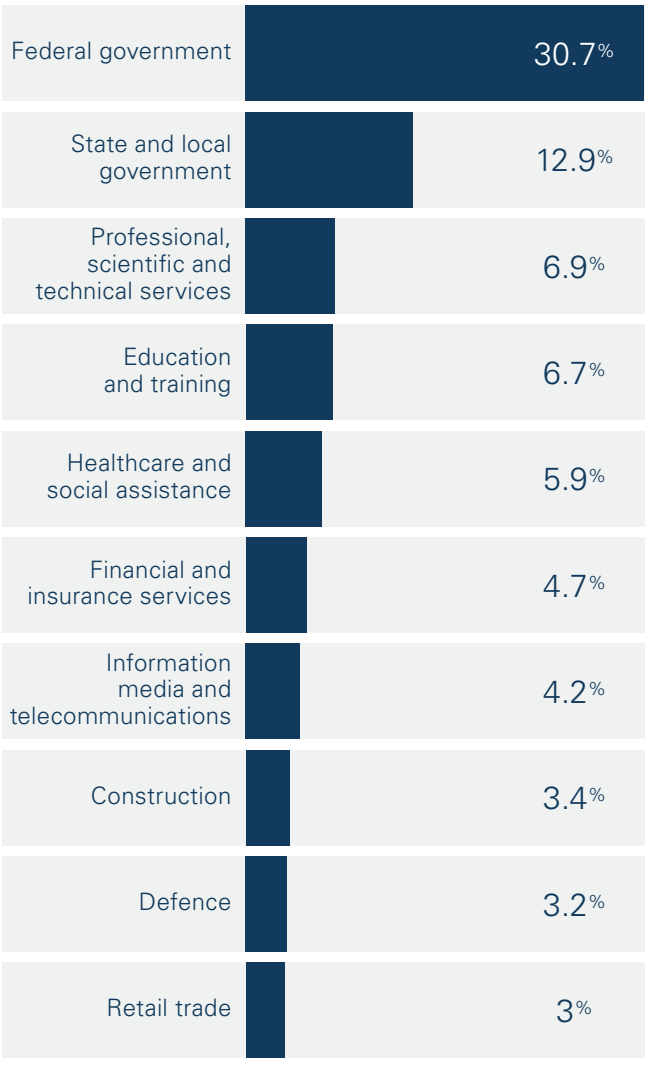
Trends in cyber security incidents

Throughout 2022-23, cyber security incidents across Australia increased. The latest data from a number of sources point to the prevalence of cyber incidents and how they are impacting organisations, as well as several emerging trends.

During the 2022-23 financial year, over 94,000 cybercrime incidents were reported to law enforcement – an increase of 23% from the previous financial year. The Australian Cyber Security Centre (**ACSC**) responded to over 1,100 of those incidents from Australian entities.

Industries most affected by cyber attacks

The federal, state and local government sectors reported the highest number of cyber security incidents in the 2022-23 financial year. Professional, scientific and technical services, educational and training and health care and social assistance were the sectors that reported the next highest number of incidents.



Commonwealth of Australia 2023, Australian Signals Directorate, 2022–23 ASD Cyber Threat Report, p9.

Notifiable data breaches

The Office of the Australian Information Commissioner (**OAIC**) publishes reports on notifications received under the notifiable data breach scheme twice a year.

Between January and June 2023, there were 409 breaches notified to the OAIC, 42% of which were cyber security incidents. Of those, according to the OAIC, 31% resulted from ransomware attacks, 29% from compromised or stolen credentials and 19% from phishing. 26% are the result of human error.

Access to sensitive information and data

21% of notifiable data breaches involved access to health information and other sensitive information.

Most notifiable data breaches (88%) involved contact information, such as an individual's name, home address, phone number or email address.

Identity information was exposed in 60% of notifiable data breaches and included an individual's date of birth, passport details and driver licence details.

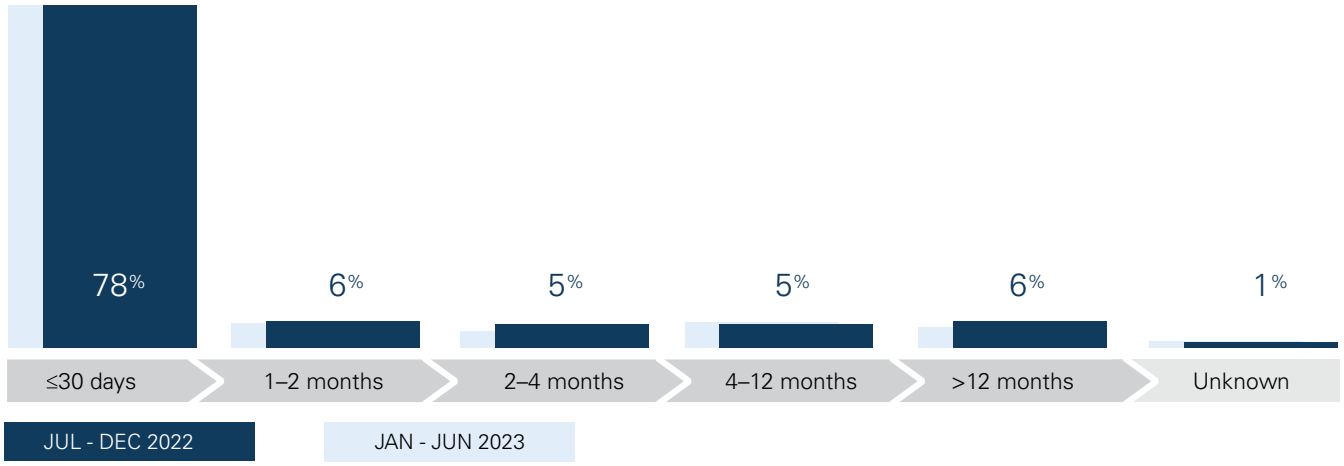
15% of notifiable data breaches involved access to financial details.

Commonwealth of Australia, Office of the Australian Information Commissioner, Notifiable Data Breaches Report: January to June 2023.

Time taken to identify breaches

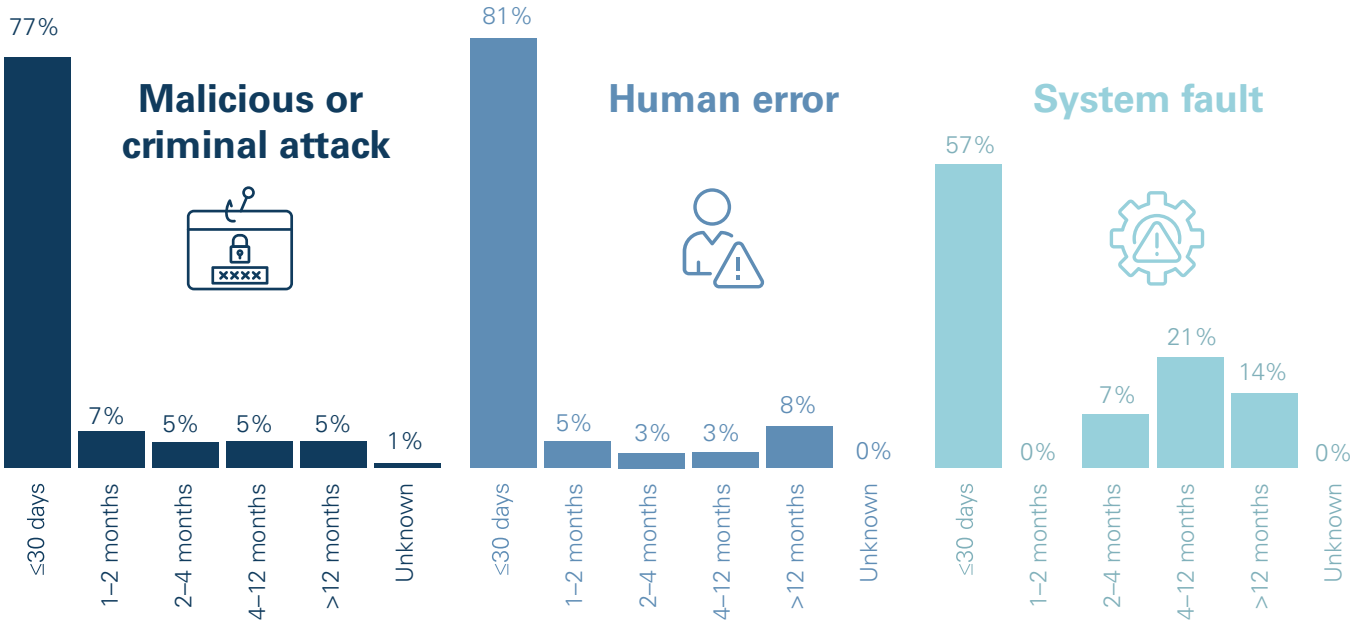
78% of breaches were identified within 30 days of occuring.

The time taken by entities to identify breaches has tended to vary depending on the source of the breach. Breaches caused by human error or malicious or criminal attacks are generally the fastest to be identified, while breaches caused by system faults are generally the slowest to be identified.



Commonwealth of Australia, Office of the Australian Information Commissioner, Notifiable Data Breaches Report: January to June 2023.

Time taken to identitfy breaches by sources of breach



Commonwealth of Australia, Office of the Australian Information Commissioner, Notifiable Data Breaches Report: January to June 2023.

Cyber attacks and data exfiltration

According to Sophos' State of Ransomware 2023 research, in 30% of attacks where data was encrypted, data was also exfiltrated. 84% of ransomware attacks include data exfiltration.[1]

1 Coveware Ransomware Quarterly Report Q4 2021.

Ransomware variants

Ransomware is a common and dangerous type of malware that works by locking or encrypting files so an organisation can no longer access them.

The ACSC has created 'profiles' on several ransomware variants, including Conti, Royal, ALPHV (aka BlackCat), Lockbit 3.0 and Lockbit 2.0, suggesting they are the most common ransomware variants in Australia (or at least the most dangerous). The 'profiles' detail the threat level of each ransomware variant and outline tactics, techniques and procedures for mitigating harm.

Conti – First detected in early 2020, Conti is a ransomware-as-a-service (RaaS) affiliate program associated with Russian-speaking cybercrime actors.

Royal – First observed in September 2022, used by cybercriminals to conduct ransomware attacks against multiple sectors and organisations worldwide, including Australia.

ALPHV (BlackCat) – First detected in late 2021, ALPHV (aka BlackCat, Noberus) is a RaaS affiliate program associated with Russian-speaking cybercrime actors.

Lockbit 3.0 – First discovered in March 2022, Lockbit 3.0 ransomware encrypts files on compromised computer systems and makes them inoperable. Victims receive instructions to initiate ransom negotiation with the threat actors.

Lockbi 2.0 – LockBit (aka LockBit 2.0, ABCD) is a ransomware variant first detected in September 2019, used by cybercriminals targeting multiple sectors and organisations around the world, including Australia.

Ransom payments and demands

Historically, ransoms have been paid in 20% of cyber incidents. This has declined over the last few years to around 10-15%.

53% of Australian organisations surveyed in a global ransomware survey confirmed that they paid the ransom following a ransomware attack.

A 2022 study published by the Australian Institute of Criminology found that 23.2% of small to medium-sized business owners paid the ransom demanded by the attacker. 39.7% of owners that paid the ransom largely did so based on advice they received, 35.9% because they did not have insurance and 34.9% because they could afford the ransom.

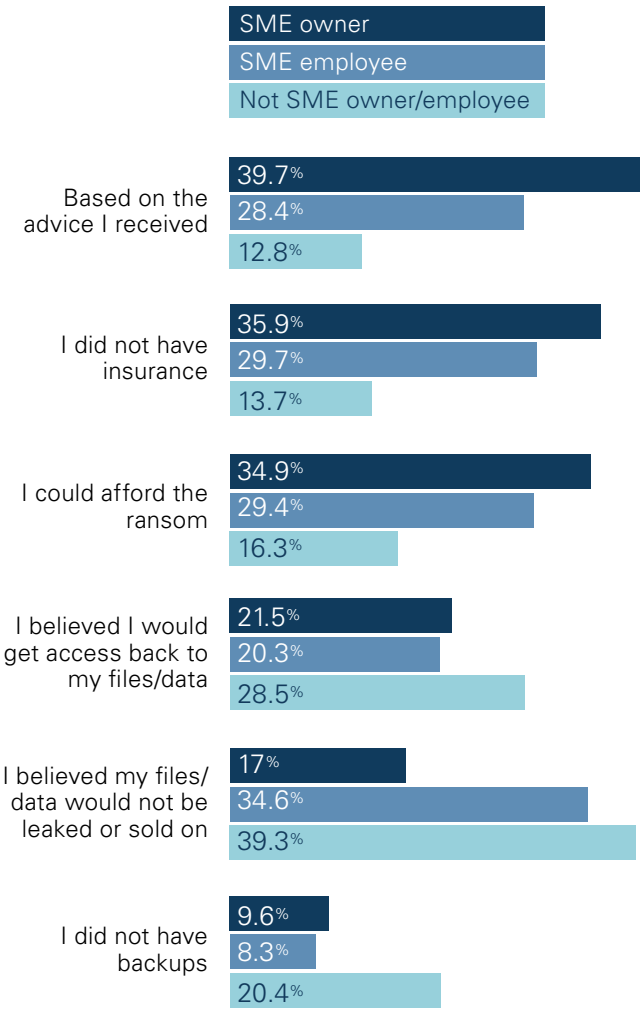
Ransom payments made to threat actors

Based on a report from 2022, on average, Australian organisations pay $250,000 per ransomware attack.

A 2022 study published by the Australian Institute of Criminology found that medium-sized businesses (defined by the Australian Bureau of Statistics as between 20 and 199 employees) had the highest average loss per cybercrime report where a financial loss occurred.

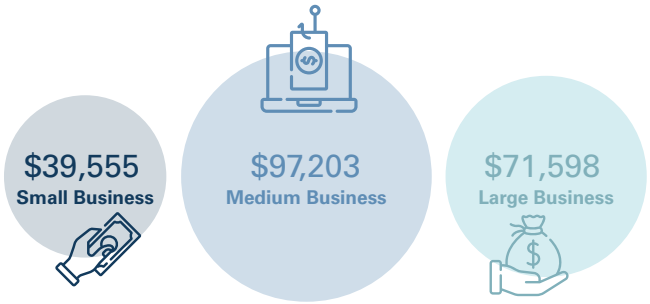
Russia is a major hub for advanced cybercrime gangs. It is reported that 74% of all money raised in ransomware attacks went to Russia-based groups.

Reasons for paying the ransom among past-year ransomeware victims



Commonwealth of Australia, Australian Institute of Criminology, Statistical Bulletin 35 October 2021, p12.

Cybercrime reports and average reported loss by organisation size for financial year 2022-23



Commonwealth of Australia 2023, Australian Signals Directorate, ASD Cyber Threat Report 2022-2023, p44.

Cryptocurrency used in ransomware demands

At the epicentre of the escalation of ransomware attacks, cryptocurrency is a digital currency secured by cryptography and based on blockchain technology. It is hard to trace, making it ideal for ransomware demands. Enormous payments have been requested, usually in cryptocurrency, in return for the promise of non-publication of sensitive data. Cyber criminals often demand ransom in cryptocurrency.

Provision of functional decryption keys and/or evidence of data deletion

76% of ransomware attacks involve cybercriminals successfully encrypting the data of the organisation being attacked.

The business and professional services industry suffers the highest frequency of data encryption (92% of attacks resulting in data encryption). All Australian organisations surveyed in a global ransomware survey that had paid the ransom following an attack were able to recover their data.

Should organisations pay a ransom?

The ACSC advises that organisations should never pay a ransom, as there is no guarantee this will result in regaining access to information, nor prevent information from being sold or leaked online. This may also lead to an organisation being targeted by another attack.

In November 2022, the Minister for Home Affairs and Cyber Security confirmed that the Federal Government was considering introducing laws that would make it illegal to pay ransoms demanded by cyber criminals.

While the advice remains consistent from the ACSC that organisations should never pay a ransom, there is still the open question of whether a ban on ransom payments would be affected through civil or criminal law.

Further, under certain circumstances, it may already be illegal for Australian organisations to pay a ransom, such as if the payment funds further criminal or terrorist activity of groups sanctioned by the United Nations.

Mandatory breach reporting trends

Organisations face an increasingly complex kaleidoscope of regulatory obligations regarding cyber security. In this section, we discuss mandatory data breach reporting obligations in Australia, including those that are sector or asset-specific, and explore trends from across multiple regulators, including recent proposed privacy and data protection law reforms.

Privacy Act reporting obligations

Under the *Privacy Act 1988* (Cth) (**Privacy Act**), an entity (an organisation or agency) is obliged to notify the OAIC and affected individuals where the entity suffers an 'eligible data breach', unless an exception applies.

An 'eligible data breach' is taken to have occurred in relation to an entity where:

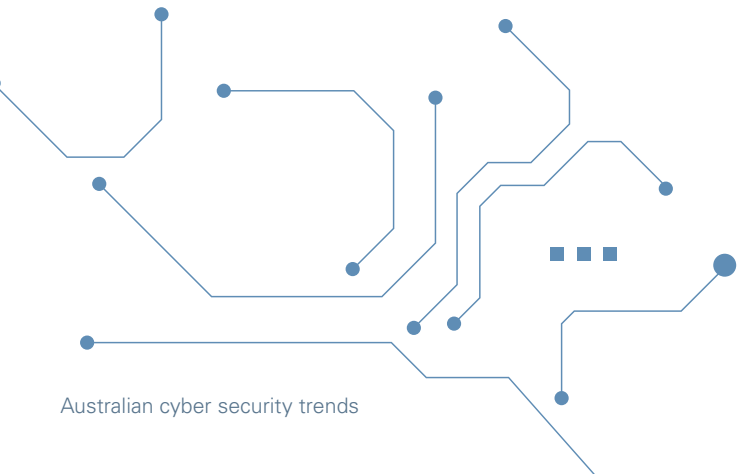
- there is unauthorised access to or disclosure of personal information 'held' by the entity; and
- a reasonable person would conclude that the unauthorised access or disclosure would be likely to result in serious harm to one or more individuals to whom the information relates.

However, if the entity is able to take remedial action in relation to the access or disclosure and such action is taken before the access or disclosure results in serious harm and a reasonable person would conclude that the access or disclosure would not be likely to result in serious harm to any of those individuals to whom the information relates, then there is no eligible data breach.

The OAIC publishes reports on notifications received under the notifiable data breach scheme twice a year. The report noted that between January and June 2023, there were 409 breaches notified to the OAIC.

As in other jurisdictions, including Canada, the leading cause of notifications to the OAIC are data breaches resulting from malicious or criminal attacks, which accounted for 70% of all notifications.

Further, the health sector continues to report the most notifiable data breaches, followed by the finance, recruitment, legal, accounting and management services and insurance sectors, respectively.



Proposed reforms to the notifiable data breach scheme

On 28 September 2023, the Federal Government released a response to the Attorney General's Privacy Act Review Report (**Report**). The response indicated the Government's positions regarding the expansive list of reforms to the Privacy Act proposed by the Report and its intention to strengthen and modernise privacy protections for Australians.

There are a number of proposed reforms related to the notifiable data breach scheme. One such proposal is a new 72-hour timeframe for entities (subject to the Australian Privacy Principles under the Privacy Act) to report eligible data breaches to the OAIC after they become aware that there are reasonable grounds to believe an eligible data breach has occurred. This change, which the Federal Government has agreed to in-principle, imposes a tighter timeframe in which to report eligible data breaches to the OAIC – the current timeframe is 'as soon as reasonably practicable'. It would bring Australia's notification window in line with the equivalent requirement under the EU's General Data Protection Regulation (**GDPR**).

The Federal Government has also agreed in-principle with the proposal to introduce a distinction between the concepts of a 'processor' and a 'controller', which would apply to the notifiable data breach scheme. The Report notes that this would assist with addressing the confusion surrounding which party makes notifications in the event of a multi-party data breach. The Report suggests that processors and controllers would share the responsibility of notifying the OAIC, but only controllers would be required to notify affected individuals in the event of an eligible data breach.

Further, the Federal Government has also agreed in-principle to the recommendation to extend mandatory data breach reporting obligations to certain entities that are currently exempt from complying with the Australian Privacy Principles, including media organisations and employers (in relation to employee records). However, the requirements that would be imposed on these currently exempt entities may differ from the requirements imposed under the notifiable data breach scheme. For example, the proposed reforms contemplate a carve out that would exempt media organisations from notifying an affected individual, if the public interest in journalism outweighs the interest of the affected individual.

APRA standards and reporting obligations for financial institutions

The Prudential Standard CPS 234 Information Security (**CPS 234**) was introduced on 1 July 2019 and is a mandatory regulation issued by the Australian Prudential Regulatory Authority (**APRA**). It requires regulated organisations to take measures to be resilient against information security incidents (including cyber attacks) by maintaining information security capabilities commensurate with information security vulnerabilities and threats.

APRA-regulated entities include financial institutions such as authorised deposit-taking institutions (i.e. banks), general insurers, life companies and private health insurers.

Under CPS 234, APRA-regulated entities must promptly notify APRA of material information security incidents. During the 2022-23 financial year, APRA received 189 notifications, an increase from the 116 notifications received in 2021-22.

On 2 February 2023, APRA published its supervision and policy priorities, which set out APRA's priorities for the following 12 to 18 months.One of APRA's key supervision priorities for 2023-24 is to improve cyber resilience by:

- undertaking detailed assessments and rigorous pursuit of CP 234 breaches;
- requiring and reviewing comprehensive remediation plans to ensure timely rectification and follow up of all gaps identified;
- conducting targeted deep-dive reviews on areas of weakness that fail to meet expectations; and
- sharing insights and industry-wide guidance to direct cyber resilience uplift.

Organisations' obligations also extend to their external service providers.

Security of critical infrastructure obligations

The *Security of Critical Infrastructure Act 2018* (Cth) (**SOCI Act**) aims to provide a framework for managing risks relating to Australia's critical infrastructure assets and systems of national significance. Since 2021, the SOCI Act has undergone extensive amendments which have expanded the number of business and industries subject to the SOCI Act from four to 11. It also introduced new reporting and notification obligations for owners and operators of critical infrastructure assets, including mandatory reporting obligations for cyber incidents in relation to critical infrastructure assets.

Under section 30BC of the SOCI Act, if the responsible entity for a critical infrastructure asset becomes aware that a cyber security incident has occurred, or is occurring, and that the incident has had, or is having, a **significant impact** on the availability of the asset, the responsible entity must notify the ACSC within 12 hours after becoming aware of the incident. A significant impact is where the asset is used in connection with the provision of essential goods or services and has materially disrupted the availability of those goods or services, or if any of the circumstances specified in the rules exist in relation to the incident.

Under section 30BD of the SOCI Act, if a responsible entity for a critical infrastructure asset becomes aware that a cyber security incident has occurred, is occurring or is imminent and has had, is having, or is likely to have, a **relevant impact** on the asset, they must notify the ACSC within 72 hours after becoming aware of the incident. A 'relevant impact' is an impact (whether direct or indirect) on the availability, integrity, reliability or confidentiality of the asset.

Cyber security and directors' duties

Cyber security must remain an important consideration in the boardroom. Australia's 2023-2030 Cyber Security Strategy calls for an uplift in cyber security standards that will likely have sweeping effects on boardroom practices and governance frameworks in Australia.

Directors' duties

There are a number of directors' duties under the *Australian Corporations Act 2001* (Cth) (**Corporations Act**). Under section 180, directors must exercise their powers and perform their duties with the degree of care and diligence that a reasonable person would exercise if they:

- were a director or officer of a corporation in the corporation's circumstances; and
- occupied the office held by, and had the same responsibilities within the corporation as, the director or officer.

In interpreting the scope of these duties, the Courts have established certain minimum standards of care that are expected of all directors. For example, a director must:

- acquire a basic understanding of the business;
- be continually informed about the activities of the company; and
- generally monitor the business's affairs.

In assessing whether a director has contravened their duty of care, the Court will attempt to 'characterise' the director according to the reasonable standard of care – that is, the Court will identify what the director ought to have done with reference to existing case law, general industry practice and established standards (such as those described above).

Managing cyber security is increasingly falling under the umbrella of directors' duties.

The outcomes of Australia's 2023-2030 Cyber Security Strategy are likely to shape the scope of directors' duties by establishing best practice cyber security standards, which directors must consider in fulfilling their duties.

Cyber in the boardroom

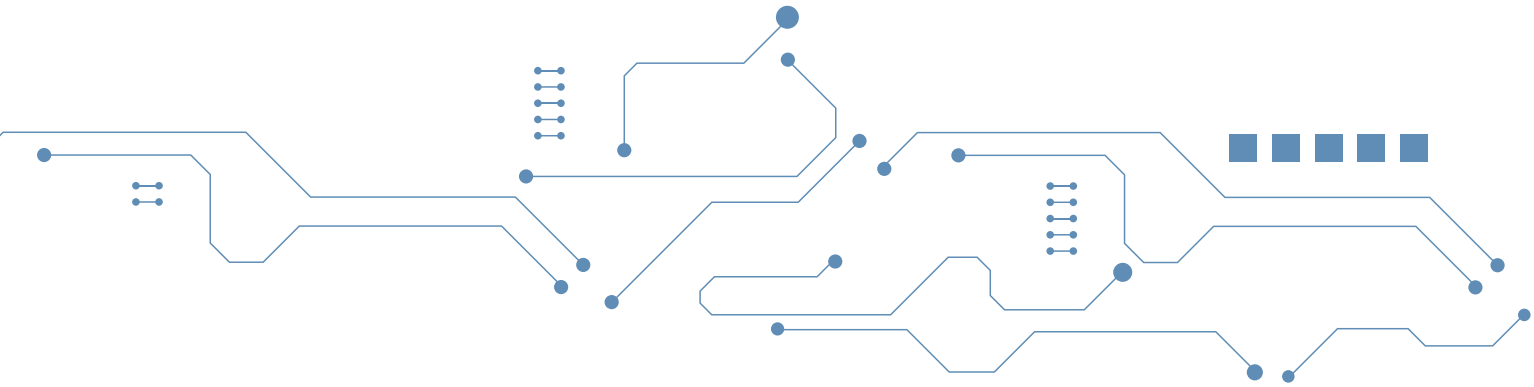
The Australian Securities and Investments Commission (**ASIC**) has stated that the directors' duties under the Corporations Act may govern directors' management of a company's cyber risks. The 2023-2030 Cyber Security Strategy reiterates the Australian Government's call for input regarding its 2021 *Strengthening Australia's Cyber Security Regulations and Incentives Discussion Paper* for the creation of best practice cyber security standards, to refine and clarify the role of directors in this arena.

There may be two potential governance standards:

1. **Voluntary governance standards** – for larger businesses describing the responsibilities and processes for managing cyber security risk.
2. **Mandatory governance standards** – which larger businesses would need to comply with within a specific timeframe.

However, the specific mechanisms by which these standards will come into being are still being considered. It is yet to be determined whether these standards will be formulated in legislation or through regulator guidance (i.e. interpreting the existing director duty obligations).

In any event, the creation of such governance standards will likely affect the application of directors' duties by shaping the scope of reasonable conduct that is expected of directors in respect of managing cyber security risks. In particular, the standards will assist the Courts in defining the types of cyber risk failures that may constitute a breach of directors' duties, including in relation to broader corporate disclosure obligations and duties to act in the best interests of the company and for a proper purpose.



Class actions, litigation and regulatory and enforcement trends

Class action, litigation and enforcement risks arising out of cyber incidents and data and privacy breaches are likely to increase as the Federal Government reforms the Privacy Act and focus turns to potential vulnerabilities in supply chains. In parallel, ASIC and the OAIC have signalled increasing focus on regulatory investigations and enforcement action following cyber incidents.

Data breach class actions trends

Recently, we have seen an unprecedented number of data breach class actions, following a series of high-profile, large-scale Australian data breaches in 2022 and 2023.

There have been a number of Australian data breach class actions recently, including:

- a consumer class action filed against Optus in the Federal Court in relation to the data breach announced by Optus on 22 September 2022;
- two consumer class actions filed against Medibank in the Federal Court following the data breach announced by Medibank on 13 October 2022, which have subsequently been consolidated; and
- a shareholder class action filed against Medibank in the Victorian Supreme Court.

In the absence of any tort for interference with privacy, the consumer class actions have pleaded breach of contract (failure to comply with data-handling and cyber security statements, policies and terms and conditions) and misleading representations, amounting to a breach of the Australian Consumer Law. **These class actions are widely considered to be test cases**, especially in relation to novel questions of the 'baseline' or standard of cyber resilience set by the current (largely) principle-based regulatory regimes and the establishment and quantification of loss and damage flowing from a data breach.

The shareholder class action filed against Medibank is premised on an alleged breach of Medibank's continuous disclosure obligations and non-compliance with CPS 234 (which is not prescriptive). The outcome of this class action will be significant for listed companies in assessing the risk of future shareholder class actions.

There are reports that a further consumer class action is being investigated following the cyber incident announced by Latitude Financial on 11 April 2023.

One development of interest in the data breach class action landscape was the decision by Justice Beach of the Federal Court on 12 May 2023 to stay the second data breach class action brought by consumers against Medibank. This resulted in the consolidation of the class actions. Justice Beach observed that "the court is vexed if not plagued by competing class actions" and "perhaps the court has to take a more robust approach". Justice Beach's decision may dissuade plaintiff firms from bringing competing class actions following data breaches.

Proposed introduction of a direct right of action and a statutory tort

Australia's privacy legislative landscape does not currently include a direct right to seek compensation for breaches of the Privacy Act or recognise any broader tort for invasion of privacy.

Australians currently have limited avenues to seek compensation for interferences with their privacy that constitute breaches of the Privacy Act. At present, they can:

- lodge a complaint, either as an individual or as a member of a class of affected persons, with the Information Commissioner (**Commissioner**), who may award compensation for the breach in the event that the Commissioner is satisfied that a breach of the Privacy Act has occurred; or
- apply to the Federal Court[2] for injunctive relief to restrain breaches of the Privacy Act.

There is no other enforceable right of action in Australia for breach of privacy.

2 We use 'Federal Court' to refer to the Federal Court and to the Federal Circuit and Family Court of Australia, which have jurisdiction to determine alleged breaches of the Privacy Act.

In the absence of any right to seek compensation for loss or damage suffered as a result of an interference with privacy, there have only been two privacy claims filed in Australia:

1. A class action filed against the NSW Health Administration Corporation alleging breaches of statutory obligations, breach of employment contract, equitable breaches of confidence, breaches of the Australian Consumer Law and a novel claim for tortious invasion of privacy.[3] That representative action settled in 2019 for $275,000 on behalf of 130 class members.
2. A privacy claim filed in June 2023 by a self-represented litigant against Latitude Financial Services Australia Holdings Pty Ltd for breaches of the Privacy Act in relation to the Latitude data breach.[4] That claim is currently in the interlocutory stages.

However, the Attorney-General's Privacy Act Review Report (**Report**) proposes the introduction of a direct right of action for breaches of the Privacy Act and a statutory tort for serious invasions of privacy that fall outside the scope of the Privacy Act. The Government has announced its in-principle support for the proposal.

The Report proposed reforming the Privacy Act to introduce a direct right of action for individuals or groups of individuals who have suffered loss or damage (including humiliation or injury to the person's feelings) to apply to the Federal Court for compensation for breaches of the Privacy Act. To minimise the risk that the Federal Court would be inundated by claims, the Report recommends that this direct right only be available where a claimant has made a complaint to the Commissioner and that complaint has been assessed as unsuitable for conciliation by the OAIC or by a recognised External Dispute Resolution scheme.

The Government will now undertake a further process of stakeholder engagement and impact analysis regarding the proposal, before any final decision is made as to its implementation.

The Report has also proposed, and the Government has agreed in-principle with, the introduction of a statutory tort for 'a serious intrusion into seclusion or a serious misuse of private information' that falls outside the scope of the Privacy Act. It is proposed that a plaintiff be required to establish four limbs of the tort:

- the invasion of privacy was serious;
- the claimant had a reasonable expectation of privacy;
- the invasion of privacy was committed intentionally or recklessly (not merely negligently); and
- the public interest in privacy outweighs any countervailing public interest.

The Government intends to consult with states and territories regarding potential implications for their courts and agencies, and with media organisations regarding safeguards for public interest journalism before any final decision is made on the implementation of this reform.

Litigation trends

The high-profile data breaches in 2022 and 2023 have heightened Australians' awareness of data breaches. Significantly, this coincides with increased community expectations of their privacy rights. The OAIC's survey of 1,653 Australians aged over 18 published in August 2023[5] revealed that:

- 62% of participants consider that protecting their personal information is a major concern;
- 47% of participants in the survey had been informed by an organisation that their personal information had been involved in a data breach in the previous 12 months;
- 76% of the participants whose data was involved in a data breach reported that they had experienced harm as a result, including an increase in scams, spam texts or emails (52%); emotional or psychological harm (12%); financial or credit fraud (11%) or identify theft (10%); and
- 89% of participants believed that they should be entitled to seek compensation in the Australian courts for a breach of privacy.

A 'baseline' of cyber resilience

Australia has seen significant reform in cyber security regulation over the past three years, notably under the SOCI Act. While the reforms remain predominantly principles-based, we are seeing a trend where businesses are encouraged to adopt cyber security risk management programs and establish systems for compliance with frameworks equivalent to the ISO/IEC 27001:2015, CPS 234 or the ACSC's Essential Eight Maturity Model.

In previous enforcement action taken by ASIC, the regulator contended that publicly available (but not mandatory) cyber security guidelines, including the ACSC's Essential Eight Maturity Model, establish minimum cyber security requirements.[6]

We anticipate that plaintiff firms will seek to have the Australian courts determine whether one or more of these cyber risk management frameworks can be considered to establish a minimum standard.

3 *Evans v Health Administration Corp* [2019] NSWSC 1781.
4 *Shahriar Saffari v Latitude Financial Services Australia Holdings Pty Ltd* (NSD519/2023).
5 Office of the Australian Information Commissioner (2023), *Australian Community Attitudes to Privacy Survey 2023*.
6 *Australian Securities and Investment Commission v RI Advice Group Pty Ltd* [2022] FCA 496.

A safe harbour on the horizon?

Recently, Defence Minister Richard Marles foreshadowed a proposed cyber safe harbour regime to encourage businesses to improve sharing of data with the Australian Signals Directorate during and after a cyber incident. This proposal has the support of both the Australian Signals Directorate's Director-General and the Business Council of Australia.

Injunctive relief following data breaches

On 12 June 2023, the first injunction was granted in Australia to restrain a threat actor from placing further material from a data breach on any location on the internet (including the threat actor's leak site).[7] This injunction followed the trend in the United Kingdom over the last five years. We anticipate that injunctive relief will become a tool that Australian companies may use in responding to data breaches, to limit access to and publication in the public domain of the exfiltrated data (where appropriate).

Regulatory and enforcement trends

Since 2022, one of ASIC's strategic priorities has been supporting enhanced cyber resilience and cyber security across regulated organisations.

On 13 November 2023, ASIC's Chair reiterated that cyber security and cyber resilience must be a top priority for all organisations, including oversight of cyber security risks in supply chains.[8] On the same day, it was reported that ASIC is looking for a test case where company directors and senior executives failed to take reasonable steps to adequately prepare for cyber attacks, including making 'reasonable investments proportionate to the risks that their business poses'.[9]

Commissioner-initiated investigations

The Commissioner has wide powers, of their own initiative, to investigate an act or practice by an agency or an organisation that may be an interference with the privacy of an individual or a breach of Australian Privacy Principle (**APP**) 1. APP 1 outlines the requirements for organisations and entities to manage personal information in an open and transparent way.

The Commissioner can conduct an investigation in such manner as they see fit. The primary objective for the Commissioner in undertaking an initiated investigation is the improvement of privacy practices of the regulated community generally, and of the entities the subject of the investigation specifically.

Representative complaints

Complaints regarding interferences with privacy may be lodged with the Commissioner on behalf of individuals or on behalf of a group. For a complaint to be made on behalf of a group, or a class, the following conditions must be met:

- the class members need to have complaints against the same person or entity;
- the complaints are in respect of, or arise out of, the same, similar or related circumstances (i.e. the same data breach or cyber incident); and
- the complaints need to give rise to a substantial issue of law or fact.

Unless the OAIC is satisfied that the complainant can adequately represent the interests of the class members, the OAIC may not accept or continue with a representative complaint.

In 2015, a representative complaint was made to the OAIC on behalf of 1,300 people in immigration detention, whose embedded personal data was erroneously published by the Department of Home Affairs. In January 2021, the Commissioner ordered that the Department pay compensation for non-economic loss under five categories of non-economic loss or damage, with the quantum ranging from $500 to $20,000 depending on the severity of the impact.

On 13 September 2023, the Deputy President of the Administrative Appeals Tribunal ordered that:

- the 1,295 class members who made submissions and provided evidence of loss or damage to the OAIC within the specified timeframe are to be assessed by a scheme administrator (an independent law firm);
- the scheme administrator is to assess each class member's evidence and/or submissions and allocate them to one of six non-economic loss categories, ranging from no loss or damage through to extreme loss or damage; and
- class members who are assessed as having suffered minor through to extreme loss or damage resulting from the data breach are to be paid $500 to $20,000.

7 Order made by Hammerschlag CJ on 12 June 2023 in *Juan Jose Martinez as Trustee for the Martinez HWL Practice Trust and others v Persons Unknown* (NSW SC 2023/188190).

8 ASIC, *ASIC calls for greater organisational vigilance to combat cyber threats* (23-300MR, 13 November 2023).

9 Ronald Mizen and Paul Smith, '*ASIC to target boards, execs for cyber failures*', Australian Financial Review, 13 November 2023

OAIC civil penalty proceedings

Following a Commissioner-initiated investigation, the OAIC may commence proceedings against the entity the subject of the investigation in the Federal Court or the Federal Circuit Court, seeking an order that the entity pay a civil penalty.

Prior to 2023, the OAIC had only commenced one civil penalty proceeding. On 3 November 2023, the OAIC filed proceedings in the Federal Court of Australia against Australian Clinical Labs Limited, alleging that Australian Clinical Labs Limited failed to:

- take reasonable steps to protect the personal information of its patients from unauthorised access or disclosure (alleged breach of APP 11.1);
- carry out a reasonable and expeditious assessment of whether a notifiable data breach has occurred (alleged breach of section 26WH of the Privacy Act); and
- notify the OAIC of a notifiable data breach as soon as practicable after it became aware of reasonable grounds to believe that a notifiable data breach had occurred (alleged breach of section 26WK of the Privacy Act).

As the alleged conduct occurred prior to December 2022, the maximum civil penalty available will be $2.2 million. However, the maximum penalty for 'serious' contraventions of the Privacy Act for conduct after December 2022 is the higher of:

- $50 million;
- three times the value of the benefit obtained directly or indirectly by the body corporate and any related bodies corporate, that is reasonably attributable to the conduct constituting the contravention; or
- if the court cannot determine the value of the benefit, 30% of the body corporate's adjusted turnover during the breach turnover period for the contravention.

Proposed enhanced powers for the OAIC

In February 2023, the Attorney-General proposed:

- an expansion of the enforcement mechanisms available to the OAIC, including the introduction of a tiered approach to civil penalties and infringement notices;
- enhancement of the OAIC's investigative powers to include investigations of civil penalty provisions; and
- empowerment of the Commissioner to undertake public inquiries and reviews into specified matters on the approval or direction of the Attorney-General.

The Federal Government agreed that the OAIC should have increased enforcement powers and with the introduction of tiered civil penalty provisions. We expect that draft legislation will be released for targeted consultation in 2024.

The Attorney-General further recommended that the Government explore the feasibility of industry funding models to ensure that the OAIC is 'adequately resourced to carry out its regulatory functions and use the full suite of its enhanced regulatory powers to maximum effect'.[10] The Government has agreed in-principle that the OAIC's resourcing requirements be the subject of further work, including investigating the feasibility of an industry funding model and the establishment of a contingency litigation fund for costs orders against the OAIC.

Legal implications of responses to ransom demands

In the *Trends in cyber security incidents* section of this report, we look at the latest data around organisations' responses to ransom demands. However, there are also legal implications organisations must consider.

Current legal regime

Although ransomware payments are not specifically prohibited under Australian law, a payment may, depending on the circumstances and knowledge on the part of the victim of the threat actor, offend anti-money laundering and counter-terrorism financing legislation and Australian sanctions legislation.

This legislative framework needs to be carefully navigated in circumstances in which certain prolific threat actors include associates who are proscribed individuals or entities.

Australia's 2023-2030 Australian Cyber Security Strategy reiterated that the government 'continues to strongly discourage businesses and individuals from paying ransoms to cybercriminals'. The government acknowledged that Australian businesses require clearer advice on how to respond to ransom demands and has signposted that it will develop a ransomware playbook.

Proposed reporting obligation

The 2023-2030 Cyber Security Strategy has proposed, as one of the six 'cyber shields', a no-fault, no liability ransomware reporting obligation. It intends to co-design this legislation with industry. We expect that the government will clarify how this reporting obligation will sit alongside the current legal regime.

Cyber security insurance

In response to increasing cyber risk, demand for cyber insurance has also escalated. It is now a critical component of Australian organisations' cyber risk management strategies. Capacity is, however, limited. As a result, insurers are closely scrutinising the cyber risks of potential insureds to determine whether to underwrite a particular risk and on what terms.

Underwriting processes

As part of the process of considering whether to insure an organisation and on what terms (including as to premium), insurers have been increasingly focused on:

- the type and nature of data held by an insured;
- the security or vulnerability of an insured's IT systems;
- an insured's internal processes and procedures for handling and storing data;
- reliance on third party service providers;
- staff training on cyber security issues;
- the extent to which staff have participated in cyber incident simulations and/or tabletop cyber exercises; and
- the terms of key IT contracts (including, in particular, risk allocation and management provisions).

If organisations are not able to demonstrate that they have cyber resilience, it may not be possible for them to obtain insurance against cyber risks.

Restrictions on cover

If insurance can be obtained, there are a number of exclusions which are increasingly commonly found in cyber insurance policies which have the potential to wholly or partially curtail the scope of cover.

These include:

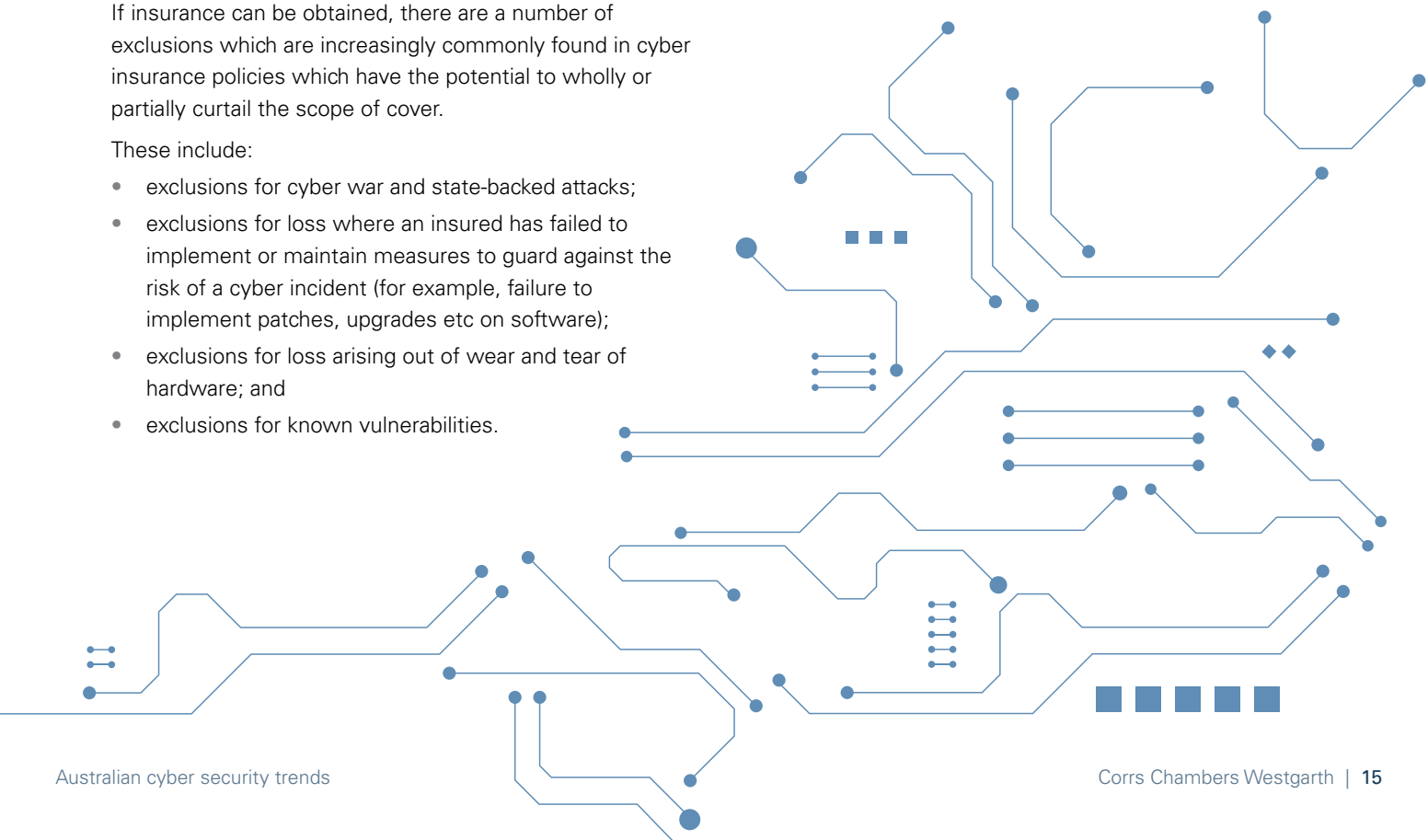
- exclusions for cyber war and state-backed attacks;
- exclusions for loss where an insured has failed to implement or maintain measures to guard against the risk of a cyber incident (for example, failure to implement patches, upgrades etc on software);
- exclusions for loss arising out of wear and tear of hardware; and
- exclusions for known vulnerabilities.

Contractually assumed liability exclusions and policy provisions which require an insured to preserve rights of recovery against third parties may be important where (as is often the case) third party IT service providers are engaged. Organisations should be cautious about assuming additional liability under IT contracts or releasing their own service providers from liability.

Further, where an insured's data is hosted by a third party service provider, the insured must ensure that the definition of 'Insured Network' (or similar) in the policy is broad enough to capture a cyber incident impacting a hosted data system.

***

It is likely that demand for cyber insurance will continue to grow. To give organisations the best opportunity to obtain comprehensive cyber insurance on reasonable terms, **they should ensure that they have robust cyber systems and processes in place.** Additionally, organisations should review the terms and conditions of their insurance policies so that they understand precisely what is covered and what is not.



Cyber security due diligence

Cyber security considerations have become a key focus area in M&A transactions, particularly where the target company holds significant customer data. Similarly, when dealing with technology service providers, customers must address the issue of the 'cyber adequacy' of the service provider and the consequences if that service provider suffers from a cyber attack.

M&A due diligence considerations

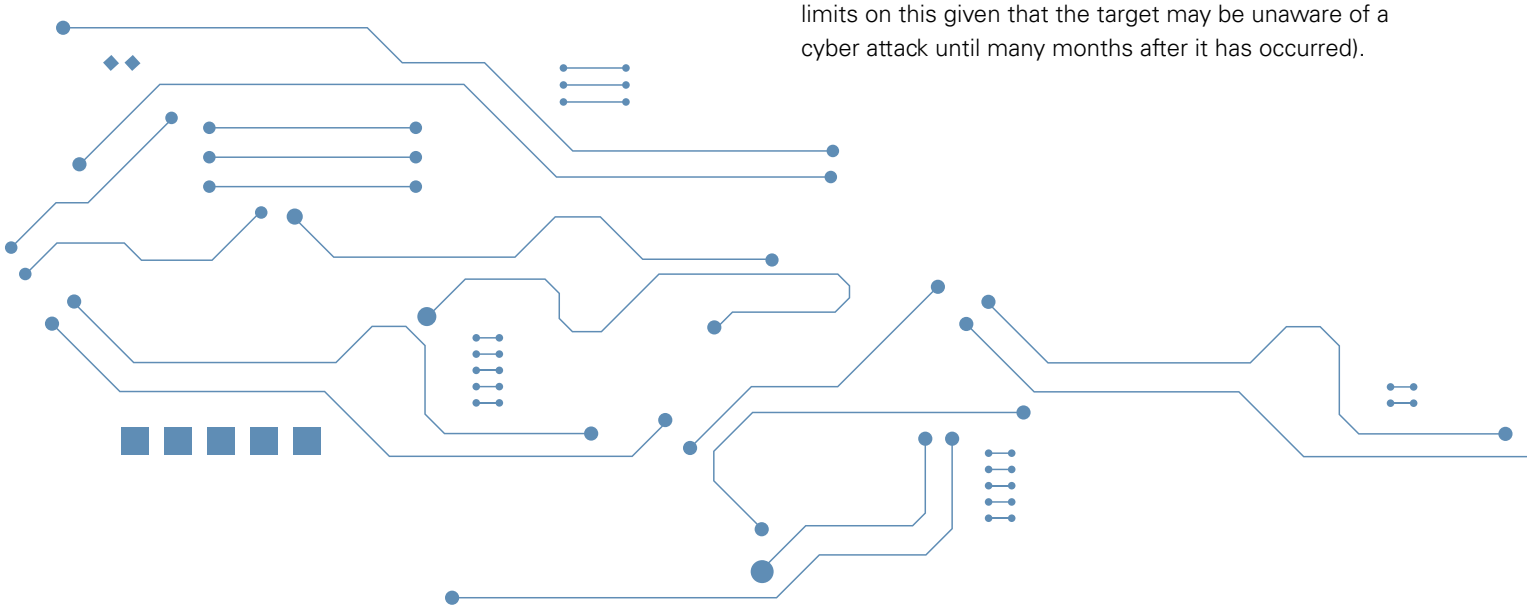
A target company's cyber resilience and historic data breaches have the potential to significantly impact the purchase price, post-completion deal value and integration strategy following an M&A transaction. In particular, a failure to identify a cyber attack in due diligence can also put the buyer's own systems at risk during the integration process.

Cyber security is becoming one of the key risks that parties focus on in due diligence, along with other issues such as staff underpayments, environmental and ESG risks. The scope of cyber due diligence may depend on a number of factors, including the deal timeline, the importance and sensitivity of data held by the target, and the extent to which the buyer is comfortable that the target has strong cyber controls in place. Due diligence may include both legal due diligence on data, privacy and cyber issues, as well as a technical review which includes cyber systems testing.

There have been many examples of buyers not identifying a pre-existing cyber issue in the target company and the target company itself was not aware of the data breach at the time of the sale. Similarly, there have been scrip-based deals where a cyber breach in the buyer has led to a significant decline in value of the scrip consideration being received by the target's shareholders and related class actions.

Some particular focus areas for buyers can include:

1. **Understanding the key data assets of the target,** with the buyer to consider the nature of the data (including sensitive information or confidential data), how that information is stored and who has access to it.
2. **Identifying applicable privacy laws** to determine whether the target's current practices comply with privacy legislation, noting that where the target has a global customer base it may be difficult to fully assess compliance with laws in every relevant jurisdiction.
3. **Understanding the target's privacy and cyber security risk management practices** and determining whether they are consistent with industry standards and best practices, and whether the target has cyber insurance in place.
4. **Considering the target's third-party arrangements,** including the company's process for undertaking due diligence on third-party suppliers, supply chain risk assessments and review of supply agreements to ensure they adequately protect the target's data.
5. **Investigating any previous or ongoing data breaches,** noting that the target should be prepared to disclose whether any breaches have occurred and, if so, how the breach occurred, what data was affected, any engagement with regulators and what changes were made in response to the breach. (However, there are limits on this given that the target may be unaware of a cyber attack until many months after it has occurred).



In addition to undertaking rigorous due diligence investigations, cyber security risks can also be mitigated for buyers by seeking appropriate warranties and indemnities in the sale agreement:

- **Warranties.** A buyer may seek warranties from the seller that the target is in compliance with all applicable privacy and data security laws. However, the sale agreement may include limitations on the buyer's ability to make warranty claims, such as financial limitations on warranties claims and exclusions for matters which are fairly disclosed in due diligence or otherwise known to the buyer.
- **Indemnities.** For specific risks identified in due diligence, a buyer may seek specific indemnities requiring the target to indemnify the buyer against certain costs incurred in connection with a historic data breach or cyber security issue.

Insurance can also help to mitigate cyber security and privacy risks in an M&A transaction. As part of due diligence, buyers should consider whether the target's existing insurance policies adequately cover cyber security risks. If warranty and indemnity insurance is being taken out to cover the buyer for losses arising from a warranty breach in the sale agreement, it may not extend to losses relating to cyber matters which are commonly excluded under these policies.

Service provider due diligence considerations

When dealing with technology service providers, customers must address the issue of the 'cyber adequacy' of the service provider and the consequences if that service provider suffers from a cyber attack. This, of course, is not limited to when the service provider's systems are affected but also when, through the use of the service provider's systems, the customer's own systems are compromised. This situation is the subject of some of Australia's most recent significant cyber attacks: it is through the use of a contractor or vendor's systems that organisations are subject to significant cyber threats.

The issue of a service provider's cyber resilience is also not limited to technology service providers – **any** service provider that is providing critical services to a customer must have cyber security diligence exercised upon them.

We have seen several legislative and regulatory requirements imposed on relevant organisations in recent times that require them to have certain processes in place with service providers to deal with service provider cyber attacks. Organisations need to put in place contractual arrangements to give effect to those processes. These include:

- **APRA CPS 234**, which requires APRA-regulated entities to assess the information security capability of certain service providers, and have controls and procedures in place relating to the protection of information assets managed by those service providers.
- **SOCI Act**, which requires owners or operators of critical infrastructure assets to have arrangements in place with certain key service providers in relation to the management and operation of services relating to those assets.

When transacting with key service providers that provide services which are technology or business critical, key provisions should be included in the contractual arrangements with such providers, including:

- a commitment to maintaining a requisite standard of information security (including through internationally recognised standards);
- a commitment to comply with certain customer specific security requirements;
- prompt reporting of any information security incidents or data breaches that may have an impact on the customer's data or systems;
- regular updates on information and system security issues experienced by the provider and implementations designed to deal with information security;
- access to relevant systems and data in the event of a security breach (including by way of escrow arrangements, if appropriate);
- appropriate redundancy arrangements in the event of a system cyber attack; and
- access to key personnel at all times required for knowledge transfer and assistance with cyber attack investigations and recovery.

However, before proceeding with any contractual arrangements, due diligence should be undertaken on the service provider to understand their cyber security resilience, their redundancy arrangements and the procedures they have in place to deal with a cyber attack. Importantly, check if they have suffered a cyber attack and how they handled it.

Contacts

Philip Catania

Partner and Chair – Data & AI, TMT Practice Group

+61 3 9672 3333 | +61 419 320 815
philip.catania@corrs.com.au

James North

Partner and Head of Technology, Media and Telecommunications

+61 2 9210 6734 | +61 405 223 691
james.north@corrs.com.au

Eugenia Kolivos

Partner and Head of Intellectual Property

+61 2 9210 6316 | +61 407 787 992
eugenia.kolivos@corrs.com.au

Mark Wilks

Partner and Head of Commercial Litigation

+61 2 9210 6159 | +61 419 387 288
mark.wilks@corrs.com.au

Chris Pagent

Partner and Head of Class Actions

+61 2 9210 6162 | +61 408 106 164
chris.pagent@corrs.com.au

Matthew Critchley

Partner

+61 3 9672 3258 | +61 413 591 014
matthew.critchley@corrs.com.au

Michael do Rozario

Partner

+61 2 9210 6566 | +61 416 263 102
michael.do.rozario@corrs.com.au

Jodie Burger

Partner

+61 7 3228 9720 | +61 458 201 947
jodie.burger@corrs.com.au

Arvind Dixit

Partner

+61 3 9672 3032 | +61 438 278 463
arvind.dixit@corrs.com.au

Frances Wheelahan

Partner

+61 3 9672 3380 | +61 419 517 506
frances.wheelahan@corrs.com.au

CORRS
CHAMBERS
WESTGARTH

Sydney
Melbourne
Brisbane
Perth
Port Moresby

corrs.com.au