RESPOND

Perspectives on
Cyber Risk 2024

MinterEllison.

Contents

Contents

The information given in this publication is believed to be accurate at the date of publication. This information may have subsequently changed or have been superseded and should not be relied upon to be accurate or suitable after this date. This publication offers a general overview of its subject matter. It does not necessarily address every aspect of its subject and we disclaim all liability to the fullest extent permitted by law. It is not intended to be, and should not be, used to replace specific advice relating to individual situations and we do not offer, and this should not be seen as, legal, accounting or tax advice. If you intend to take any action or make any decision on the basis of the content of this publication you should first seek specific advice from an appropriate professional. Some of the information in this publication may be compiled from third party sources we consider to be reliable, however we do not guarantee and are not responsible for the accuracy of such.

Introduction

Welcome to MinterEllison's ninth annual **Perspectives on Cyber Risk** 2024 report ❯

In 2024, the ever-evolving cyber landscape continues to loom large over the global economy.

Rapid advancements in new technologies, including artificial intelligence (**AI**) and machine learning (**ML**), present both opportunities and challenges for organisations – including in managing and mitigating cyber risk. Concurrently, organisations are facing a surge in the frequency and sophistication of cyber attacks; a significantly more complex and onerous privacy and data protection regulatory landscape; increasingly assertive regulators; and heightened public expectations as to how they must safeguard the ever-increasing volume of data that they collect, process and hold.

A corollary of this rapidly evolving technological and cyber risk landscape is the pressing need for organisations to implement robust data governance arrangements.

In this year's report, we analyse our ninth annual survey findings against the backdrop of a dynamically changing cyber landscape. We offer insights into recent regulatory responses, and deliver practical guidance for organisations in preparing for, and mitigating the effects of, high-impact cyber incidents.

> "Know your enemy and know yourself and you can fight a hundred battles without disaster."
>
> Sun Tzu, The Art of War

Paul Kallenbach
Partner,
Technology and data law

Susan Kantor
Special Counsel,
Technology and data law

Shannon Sedgwick
Partner,
Technology consulting, Cyber risk

1

Survey highlights 2024

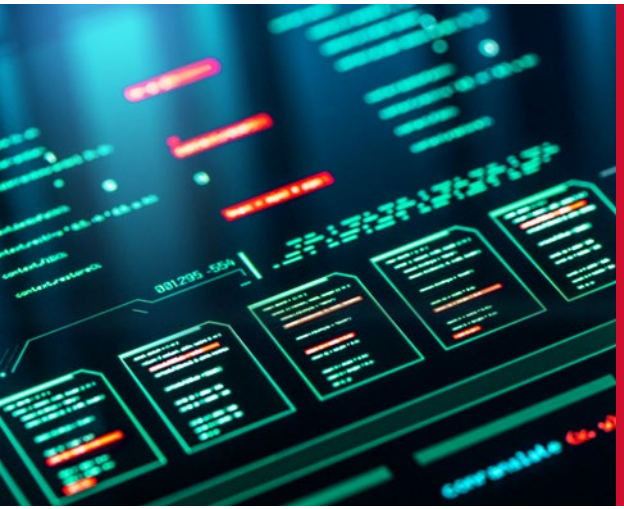
1. Survey highlights 2024

Between January and March 2024, we conducted our annual cyber risk survey, gathering insights from a broad cross-section of respondents, including CEOs, CIOs, CISOs, legal counsel, and compliance and risk managers, across diverse sectors of the Australian economy. Some of the key results are highlighted in this section.

1.1 Cyber risk is overwhelmingly a top 5 priority

In both of our previous surveys, only 56% of respondents ranked cyber risk as a 'top 5' priority within their organisations. This year, however, **72% of respondents considered cyber risk a 'top 5' priority** – likely reflecting an escalating apprehension amongst Australian organisations in the aftermath of the highly publicised Medibank and Optus data breaches of 2022.

We discuss the continuing fallout from these incidents in section 4.



16%

of respondents were the victim of a cyber attack in the last 12 months

1.2 Organisations are taking action – but there is still room for improvement

Only 16% of survey respondents reported their organisation having been the victim of a cyber attack that impacted their data or systems during the last 12 months. It may be that this low proportion is indicative of these organisations having taken proactive steps to prepare themselves for, and to mitigate the effects of, cyber attacks, by adopting a range of cyber resilience measures.

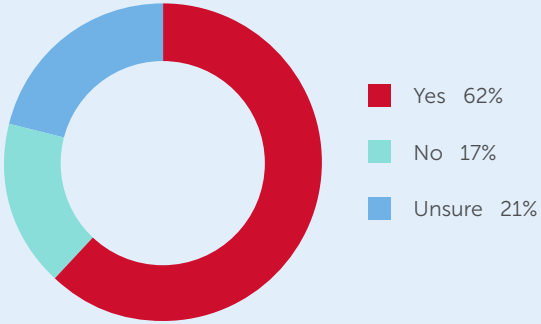
Some of the measures that surveyed organisations told us they are adopting are as follows:

- **almost 90% told us that they conduct regular cyber risk training and awareness activities**
- 62% told us that their organisations are measuring their cyber maturity against an established framework (such as the Australian Signals Directorate's Essential Eight, ISO 27001, or the National Institute Standards and Technology's cyber security framework) – up from 53% last year
- 63% of respondents told us that they tested or rehearse the plan regularly (at least annually) – up from 52% last year
- 63% told us that they thought their organisation employs sufficient resources to monitor and manage their cyber security needs effectively – up from 51% last year.

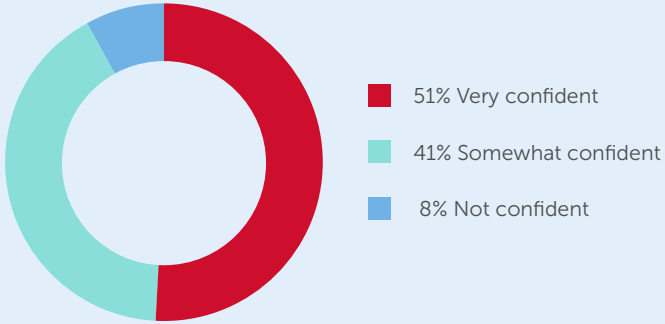
Conversely:

- only 46% of our respondents told us that they were confident that their organisation knows what data it stores, where it is stored, what controls protect it, and who has access to it – indicating the need for many Australian organisations to focus on and improve their data governance. This aspect is discussed further in section 3
- 50% of respondents told us they were either not confident, or were only somewhat confident, that they understood their regulatory and contractual obligations in the event of a cyber attack or data breach – a result that is of concern because obtaining a detailed understanding of these matters is within the control and capability of most organisations. This aspect is discussed further in section 4.

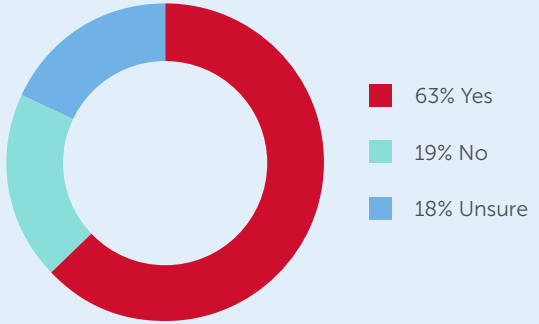
Does your organisation measure its cyber maturity against an established framework?



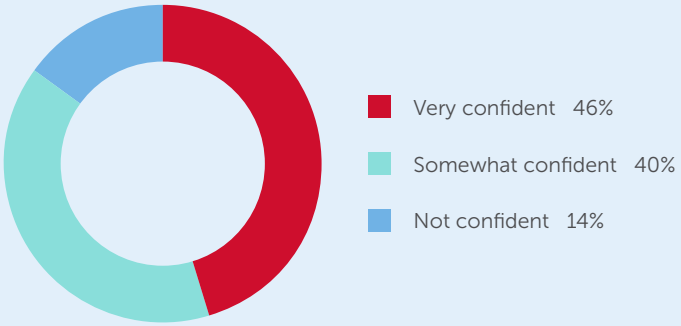
How confident are you that your organisation understands its regulatory and contractual obligations in the event of a cyber attack or data breach?



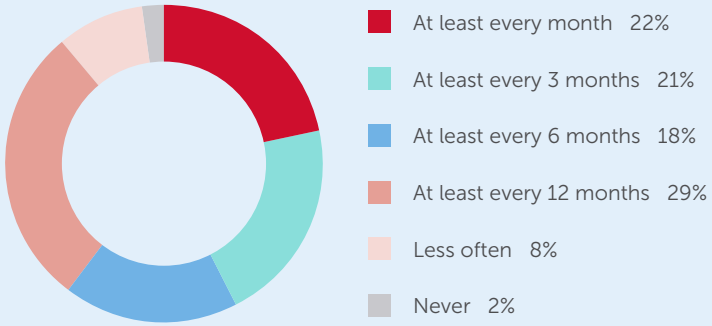
Is your organisation sufficiently staffed to monitor and manage cyber security needs effectively?



How confident are you that your organisation knows what data it stores, where it is stored, what controls protect it and who has access to it?



How often does your organisation conduct staff training or awareness activities on cyber risks?



1.3 Supply chain risk is increasing

57% of respondents told us that their third party suppliers or vendors had experienced a cyber attack or data breach in the last 12 months – underscoring the need for organisations to develop a thorough understanding of their supply chain and implement robust cyber risk mitigation strategies to address cyber threats within it. This is also a key theme in the Office of the Australian Information Commissioner's (**OAIC's**) most recent half-yearly report, in which the OAIC highlighted two specific issues for organisations to address:

- the lack of data retention and destruction provisions in supplier agreements following the cessation of services; and
- the lack of clearly defined responsibilities, as between supplier and customer, should a data breach occur, including allocation of who should assess and notify the breach.

1.4 Cyber security incident responses are still not being tested

Last year, 78% of respondents told us that they had a cyber security incident response plan in place. Pleasingly, this increased to 87% of respondents in 2024.

However, as further discussed in section 4.11 below (in the context of APRA's Prudential Standard requirements), it is critical for organisations to regularly test and rehearse their plans. This year, 63% of respondents told us that they tested or rehearse the plan regularly (at least annually). Although this is a welcome improvement against last year's 52%, it still signals there is further work to be done by many organisations to ensure that they are adequately prepared to effectively manage a cyber incident. This includes updating their plans based on the evolving threat landscape, regulatory expectations and best practice, and learning from their own and others' experiences.

1.5 Organisations are concerned about the adoption of AI

While discussions around the adoption of AI have reached fever-pitch over the last 12 months, the overwhelming majority of surveyed organisations told us that they are only somewhat confident, or are not confident at all, that their organisation is well-prepared to adopt these new technologies.

This result may well be grounded in concerns around cyber security – with **44% of respondents telling us that privacy and cyber risks were their most pressing concern in relation to the adoption of AI.** Concerns around privacy and data security as they relate to AI are well-founded, as we discuss in the next section.

"57% of respondents told us that their third party suppliers or vendors had experienced a cyber attack or data breach in the last 12 months – underscoring the need for organisations to develop a thorough understanding of their supply chain and implement robust cyber risk mitigation strategies to address cyber threats within it."

2

AI and cyber security

2. AI and cyber security

The rapidly escalating adoption of AI technologies requires corresponding measures to protect their development and use. The public's recent experience with generative AI has raised concerns around bias, safety, privacy, and the protection of intellectual property.

However, there is one aspect that has not been as widely discussed in relation to AI: the cyber security aspect. Without appropriate cyber security measures, AI technologies can be used (or abused) to amplify these and other risks.

2.1 Demystifying generative AI

Generative AI is often hyped but rarely explained. As such, an appreciation of its constituent elements is important in order to understand and manage its inherent risks (including cyber risk).

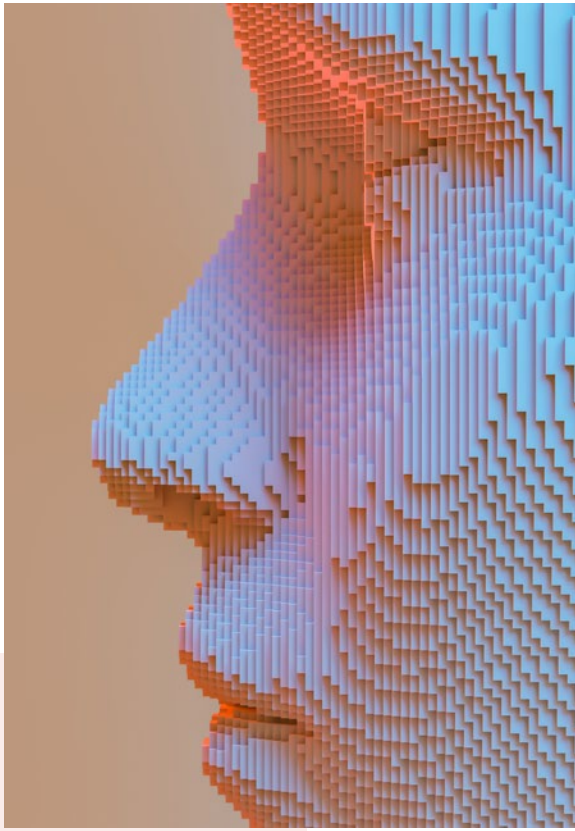
The constituent elements of generative AI are **models**, **data**, and **computing power**.

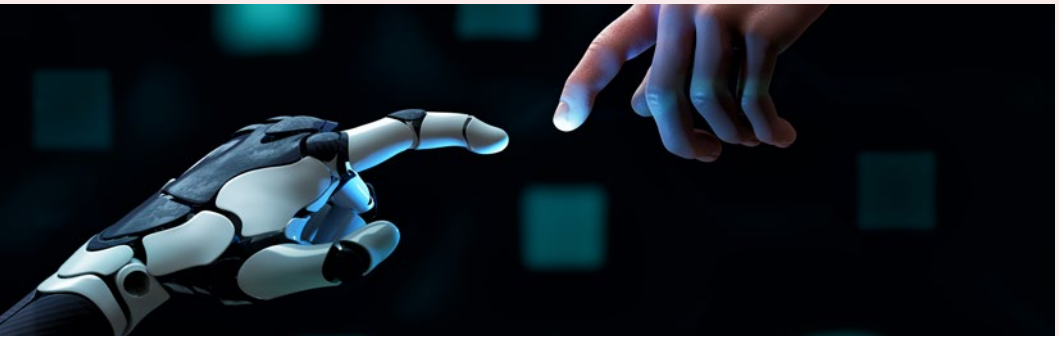
Models are the core of generative AI technology. They take inputs and produce outputs. For example, OpenAI's ChatGPT, Google's Gemini, and Microsoft's Bing are each large language models (**LLMs**), which receive text prompts and provide responses. The goal of LLMs is to produce outputs (be it text, graphics, audio or video), from given inputs, that are coherent, relevant and accurate.

Data is the information used to train a model, and the reference points from which outputs are created. Data can come from various sources, such as text, images, audio, video, sensors, and human feedback. Data quality and quantity are crucial for the performance and reliability of a model, as well as its fairness and ethical underpinnings.

Computing power is the total energy required to operate the hardware (such as CPUs, GPUs and TPUs) which involves storing data and performing calculations for a model, as well as the speed and reliability of the network connection that links the hardware, data sources, and end users.

Each of these elements – models, data and computing power – has its own distinct features and risks that must to be addressed as part of a comprehensive strategy for AI security.





2.2 Model security challenges

AI models are susceptible to being manipulated by attackers to change how they work or to access confidential information. This is called *adversarial machine learning* (**AML**). AML can affect the structure of the model, such as the mathematical values that influence how it makes decisions, or the data on which the model is trained. For example, in an LLM that generates text based on a given input, an attacker could alter the model's structure to cause it to produce offensive or misleading text, or could use the model's data to extract personal or confidential information. This can be achieved by either sending specially designed inputs to the model, known as 'prompt injections', or by direct manipulation of the model's internal functions. Researchers have recently demonstrated the use of 'AI worms', a prompt injection technique that can be used against AI email assistants to compromise sensitive information at scale. This technique involves prompting an AI model to produce another prompt in its output, which can then be scaled to infect other models through emails, compromising the content of those models.

Another aspect of model security is the protection of application program interfaces (**APIs**) that allow communication between the model and other systems or users. APIs can be exploited by malicious actors who wish to access or damage the model or the network to which it belongs. For example, an attacker could use an API vulnerability to inject malicious code into the model or steal sensitive data from the server. APIs should therefore be designed and tested with security in mind, adopting best practices such as authentication, encryption and input validation.

Finally, model security involves preventing the misuse of models by attackers who wish to deceive or harm others. For example, Microsoft has detected attacks originating from North Korea and Iran which use LLMs to create malicious phishing emails that attempt to deceive individuals into revealing their personal or financial information. Similarly, deepfake and voice mimicking technologies have recently been used to impersonate prominent figures and to spread false information (particularly within the corporate, social media and political arenas), while some models can generate code used to create viruses, ransomware or other malicious tools.

2.3 Data security challenges

Data and model security are closely intertwined, as AML attacks can exploit both the data used to train a model as well as the model itself.

One type of AML attack is 'data poisoning', which involves tampering with the training data to manipulate the model's outputs or degrade its performance. Data poisoning contrasts with prompt injection, discussed above, which targets the model's external interface by feeding it malicious inputs. Researchers have recently shown that it is possible to 'poison' the database of a generative AI email assistant using retrieval-augmented generation (**RAG**). Through either text-based self-replicating prompts or embedding a self-replicating prompt within an image file, researchers were able to steal emails containing sensitive proprietary and personal information and send spam messages within a test environment. To prevent data poisoning, datasets should be protected by conventional cyber security measures, such as identity management and access control, data classification and encryption.

Another aspect of model security unique to AI is the confidentiality of model weights, which determine how the model processes inputs and generates outputs. If model weights are compromised, they can be reverse-engineered to create alternative or open-source models which mimic or even surpass the original. This can threaten the competitive advantage of the model developer, as well as enable the misuse of the model for harmful purposes. Model weights should therefore be treated as a valuable asset of any organisation that develops and deploys custom or proprietary AI platforms.

Data privacy is a key component of lawful, responsible and secure AI use. This necessitates the protection of personal and sensitive information contained in the training data or that could be revealed by the model outputs. In particular, prompt injections could expose such information if the model is not trained or designed with appropriate privacy safeguards. To ensure privacy, a sound data governance regime (discussed in detail in section 3) is vital, including clear identification of the data assets that will be used for AI training and application, and ensuring that they do not contain sensitive or other personal information.

Finally, third party data pipelines, third party software (including open source software), and third party platforms need to be assessed for potential vulnerabilities. Many aspects of the AI supply chain will not be under the direct control of the model developer or user, and could contain vulnerabilities that allow attackers to access or manipulate data, or even the model itself. For example, if an AI model relies on a cloud provider to store and process data, the provider's security policies and practices should be carefully reviewed. Similarly, if an AI model uses an open source library or framework to perform some of its key functions, the library or framework should be updated regularly and assessed for bugs and vulnerabilities. In doing so, the risks of data breaches, unauthorised access, or malicious interference with the AI model can be reduced.

2.4 Computing security challenges

Securing the computing infrastructure (hardware, software, networks, platforms, and systems) that underpin the functioning of an AI model is vital to ensuring its reliability, continuity and scaled accessibility. This requires addressing:

- **network outages** – the disruption to or loss of connectivity within or between networks, which can affect the availability and performance of AI systems that depend on it. For example, if an AI system uses a cloud platform to store and process data, a network outage could prevent the system from accessing or updating the data, or delivering results to the end user. Network outages can be caused by natural disasters, human error, hardware failures, or malicious attacks (for example, denial-of-service (**DoS**) or distributed denial-of-service (**DDoS**) attacks, which aim to overload or disrupt a network with excessive traffic or requests);
- **risk of intercepted communications** – communications that are captured or monitored by unauthorised parties can compromise the confidentiality and integrity of AI systems that use them. For example, if an AI system uses wireless or internet connections to transmit data or commands, intercepted communications could expose sensitive or other personal information, model parameters or encryption keys, or allow attackers to alter or inject malicious data or commands, which could affect the behaviour or output of the AI system. Intercepted communications could be facilitated by weak encryption, the use of insecure protocols, or compromised devices or networks;
- **software vulnerabilities** – being flaws or weaknesses in software code or design that could be exploited by attackers to gain unauthorised access or control over an AI system or its components. For example, a compromised software library or framework could allow attackers to inject malicious code into, or modify the functionality or hijack the execution of, the AI system. Software vulnerabilities can result from coding errors, the use of outdated versions, malicious injection, or insufficient testing or validation; and
- **technical debt in computing infrastructure** – being the accumulated costs and consequences of suboptimal or incomplete technical decisions or solutions, such as using shortcuts, outdated technologies, or inconsistent standards. Technical debt can impair the quality, performance, maintainability and security of AI systems, as well as increase the complexity and difficulty of updating or fixing them. For example, if an AI system uses legacy or incompatible software or hardware components, technical debt could make it harder to patch or upgrade them, or to integrate them with newer or more secure technologies. Technical debt could also increase the likelihood of errors, bugs, or vulnerabilities in the system, or reduce its compatibility or interoperability with other systems or platforms.

2.5 Confronting AI security head-on

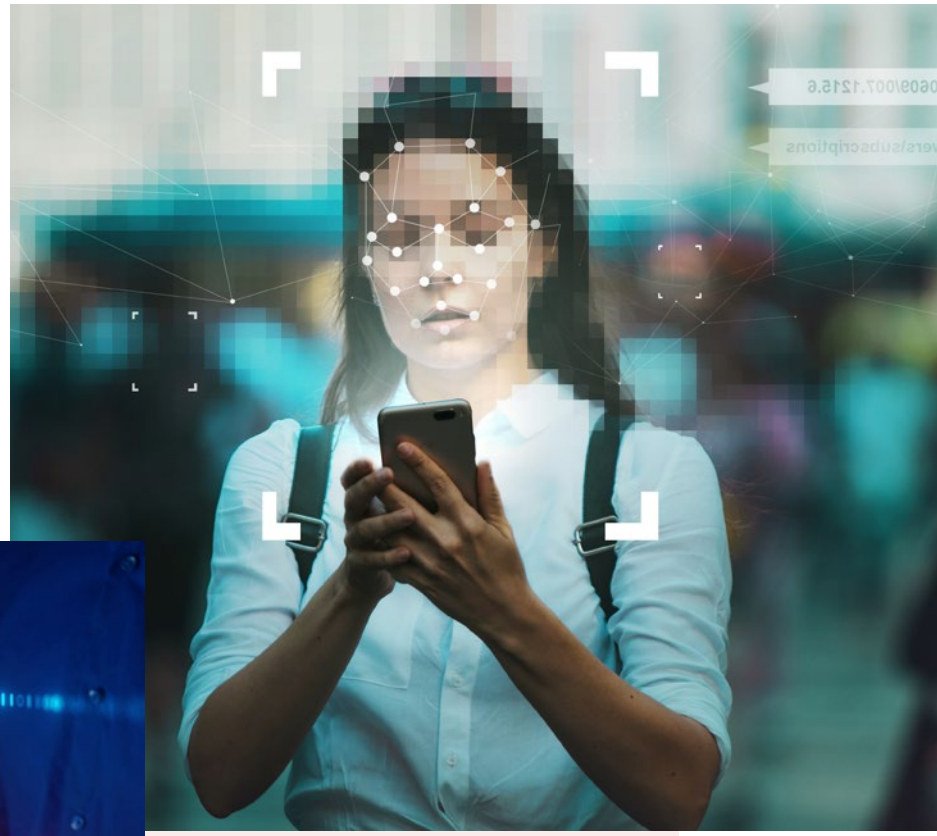
Managing the security of AI is a complex and multifaceted challenge for organisations.

AI and cyber literacy are foundational requirements, and should be calibrated to address AI's unique security risks. This should include training personnel to detect and critically reflect on the ability of LLMs to deploy deepfakes in phishing and other scams, including by undertaking sophisticated internal phishing simulations.

While training personnel to recognise and respond to the unique threats posed by AI technologies is essential, it is not, of itself, sufficient to ensure the safe and trustworthy use of these tools. Organisations also need to adopt a security-first posture that integrates AI security into every stage of the AI development and deployment lifecycle, from design to evaluation to deployment. This includes implementing robust AI governance frameworks, ethical principles, and technical standards that align with applicable law and with best practice. Moreover, organisations need to foster a culture of collaboration and transparency, both internally and externally, to share information and insights on AI security risks and mitigations. By engaging with stakeholders, regulators and peers, organisations can learn from each other's experiences and challenges, and collectively advance the state of AI security.

"

By engaging with stakeholders, regulators and peers, organisations can learn from each other's experiences and challenges, and collectively advance the state of AI security.



3

The need for enhanced data governance

3. The need for enhanced data governance

In 2024, a range of far-reaching regulatory reforms are expected, intended to change the way personal and other information is governed, managed and protected at scale in Australia.

After many years of consultation, the Federal Government has indicated it will release draft legislation that will amend the *Privacy Act 1988* (Cth) (**Privacy Act**) to provide for greater protection of personal information. In addition, following the release last year of the 2023-2030 Cyber Security Strategy (**Strategy**), the Australian Government will pursue increased regulation of business critical data, and will further clarify and refine the security of critical infrastructure laws.

Given the extent and significance of these changes, it is imperative for organisations to not only make preparation a key focus, but also to proactively engage in understanding and aligning their processes with these new laws. In particular, organisations planning to take a best practice approach to preparing for these changes should review and enhance their **data governance competencies**.

3.1 Privacy and data protection reforms

The Privacy Act reforms signify the most sweeping changes to the Privacy Act since the private sector reforms were enacted in 2001. Significantly, this includes changes to fundamental concepts under the Act (such as the definition of 'personal information' and requirements in relation to consent), as well as increased enforcement powers and a graduated set of civil penalties. These reforms are discussed further in section 4.1.

Increased data protection has also been flagged as a key focus of the further reforms to the Security of Critical Infrastructure (**SOCI**) laws, which have already seen significant expansion over the last three years. In particular, to address the increasing number of cyber incidents impacting non-personal information (such as financial records, software code and other intellectual property), the Government proposes to amend the definition of 'asset' under the SOCI laws to extend it to data storage systems that hold 'business critical data'. As a result, those systems will be treated under the SOCI laws in the same manner as physical critical infrastructure assets. The SOCI reforms are discussed in further detail in section 4.2.

3.2 Implications for organisations

These proposed reforms will have substantial repercussions for the data governance and management practices of organisations across all sectors of the Australian economy. To prepare for them, organisations will need to adopt robust data governance frameworks and processes that ensure compliance with these new laws and the protection of their data assets.

3.3 What is data governance?

Data governance is the design and implementation of the policies, standards, processes and roles that govern the collection, use, and storage of data. It defines who can access the data, how it is collected, how it can be used, and what protections apply to it. Data management is the practical execution of these policies and processes. Both are required in order to maintain good data hygiene, and will become increasingly important for organisations to achieve compliance with new privacy and data protection laws.

The three pillars of data governance are **people**, **processes** and **technology**.

People

Data governance involves assigning different roles and responsibilities to different stakeholders, usually referred to as data owners, data stewards and data custodians.

- **Data owners** are the strategic leaders of data governance. They define the vision, objectives and principles of how data should be classified, used, protected and quality-assured across the organisation.
- **Data stewards** are the operational managers of data governance. They execute the strategy and framework set by data owners and ensure compliance with data governance practices. Data stewards interact closely with specific datasets, monitoring their quality, accuracy and security.
- **Data custodians** are the technical specialists of data governance. They implement and maintain the data governance architecture, such as data standards, security measures, policies and processes. They also provide technical support and guidance to data owners and data stewards.

Processes

Data governance processes are intended to ensure the lawful, effective, secure and ethical use of data in an organisation. These processes can be grouped into three categories: data strategy; data inventory and architecture; and data standard, policies and procedures.

- **Data strategy** is the high-level vision and plan for how an organisation will leverage data to achieve its goals and objectives. It defines the business purposes and benefits of collecting, storing, sharing, and analysing data, as well as the risks and challenges involved. A data strategy should align with the overall organisational strategy and guide all data governance activities.
- **Data inventory and architecture** is the comprehensive mapping and documentation of the organisation's data assets. It includes metadata, such as data sources, types, formats, quality, ownership and access rights. It also describes the data flows within and across different business units, systems and platforms.
- **Data standards, policies and procedures** are the rules and guidelines that govern the data practices of an organisation. They specify the roles and responsibilities of data owners, stewards, and custodians, as well as the data quality, legal (including privacy) and ethical requirements that must be met. They also outline the processes and tools for data collection, storage, integration, analysis, dissemination and disposal. Best practice dictates that this documentation should embed security-by-design and privacy-by-design as foundational precepts.

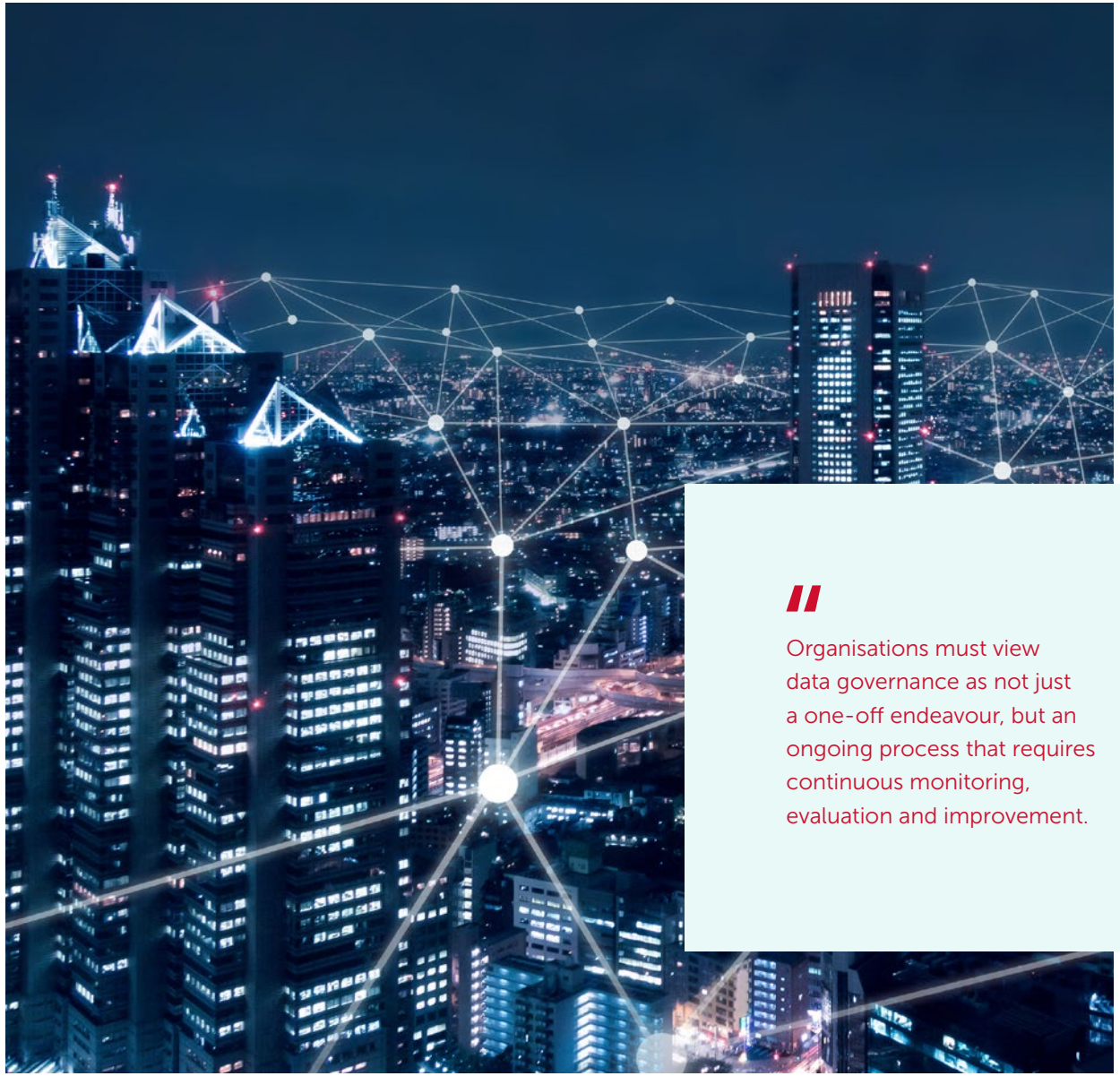
Technology

The technologies used to implement data governance must be fit-for-purpose, and sufficiently transparent as to how data is processed so that all relevant stakeholders, including senior management and executive level decision-makers, can understand the organisation's data flows.

3.4 Essential next steps

54% of our survey respondents told us that they were either 'not confident' or only 'somewhat confident' that their organisations knew what data they store, where it is stored, what controls protect it, and who has access to it. These results indicate that many organisations have much work to do if they are to adapt to, and thrive in, a rapidly evolving technological environment (discussed in section 2) as well as a rapidly changing regulatory and cyber risk landscape (discussed in section 4). This must include implementing a proactive approach to data governance that aligns with their strategic goals and values. Organisations must view data governance as not just a one-off endeavour, but an ongoing process that requires continuous monitoring, evaluation and improvement. Implementing and maintaining a robust data governance framework can help organisations to:

- enhance data quality and consistency – improving decision-making, operational efficiency, and customer satisfaction;
- strengthen data security and privacy – reducing the risk of data breaches (and resulting legal, financial and reputational damage);
- comply with their legal obligations – to support organisational accountability, trustworthiness and social responsibility; and
- leverage new technologies – by harnessing the potential, and mitigating the risks of emerging technologies, such as data analytics and AI.



> Organisations must view data governance as not just a one-off endeavour, but an ongoing process that requires continuous monitoring, evaluation and improvement.

4

Regulatory developments

4. Regulatory developments

Cyber security is a critical and ever-evolving issue for businesses, governments and consumers alike. Australian regulators have been active in proposing and implementing law reforms to enhance cyber resilience, accountability and transparency, across every sector and industry of the Australian economy. The following sections highlight some of the key legislative and policy developments that have occurred (or are underway) in the cyber security arena.

4.1 Privacy Act reform proposals

The Federal Government's ongoing review of the Privacy Act is at the heart of these regulatory reforms. On 28 September 2023, the Government released its response to the Attorney-General Department's Report on the Review of the Privacy Act (**AG Report**).

The AG Report, released on 16 February 2023, marked the conclusion of its review of the Privacy Act. One of the key aims of the review was to propose a pathway to modernise and strengthen Australia's privacy framework. The AG Report tabled 116 proposals for privacy reform. A detailed description of these proposed changes can be found in our article, The most sweeping reforms to Australian privacy law in over twenty years.

The Government's response identifies the following key focus areas for reform of the Privacy Act:

Bringing the Privacy Act into the digital age

A central theme of the AG Report is the need to bring the Privacy Act into the digital age, given the rapid and constant evolution of technology, which has enabled new ways of collecting, using and disclosing personal information. The Government has expressed its in-principle support for several proposals to make the Privacy Act more relevant and effective in the digital context. This includes broadening the definition of 'personal information' to include IP addresses, device identifiers, location data, and other technical information that can be used to identify or infer an individual's identity. Importantly, this would align the Privacy Act with the European Union's General Data Protection Regulation (**GDPR**) and other international privacy frameworks.

Uplifting protections

Another key objective of the Government's response is to uplift protections under the Privacy Act. The Government recognises that the public now expects a significantly higher level of security and accountability from entities that collect, use, hold and disclose their personal information, particularly following the Medibank and Optus data breaches of 2022.

To enhance the security of personal information, the Government has agreed to amend the Privacy Act to specify that the 'reasonable steps' that an organisation must include technical and organisational measures. (**APP**) 11 requires organisations to protect personal information from misuse, interference, loss, unauthorised access, modification or disclosure. The Government has also agreed that the OAIC should provide further guidance on the 'reasonable steps' to assist organisations in implementing best practice and complying with their legal obligations.

The Government has also proposed enhancements to the Notifiable Data Breaches (**NDB**) scheme, which requires organisations to notify the OAIC and affected individuals of eligible data breaches. It has agreed in-principle to introduce new organisational accountability obligations to encourage entities to integrate privacy-by-design into their operating procedures. This means **organisations will have to demonstrate how they embed privacy safeguards and principles into their data processing activities, such as by conducting privacy impact assessments and appointing privacy officers**. The Government has also agreed in-principle to truncate the notification timeframes for eligible data breaches. Organisations previously had up to 30 days to complete their assessment of a data breach and were required to issue notifications as soon as practicable thereafter. **Going forward, the timeframe for notification will be drastically reduced, to 72 hours**, which also aligns with international practice and other Australian notification laws, such as the SOCI laws and the APRA prudential standards.

The Government's report also discussed the use of **high privacy risk activities**, such as facial recognition technology and the collection of biometric information. The Government has agreed that further consideration is needed to determine how these activities should be addressed under the Privacy Act, given the potential for serious privacy intrusions and the lack of adequate regulation. The Government has indicated that it will consult with stakeholders and experts on the appropriate regulatory framework for these activities, and whether additional protections or consent requirements are necessary.

> "
>
> This means organisations will have to demonstrate how they embed privacy safeguards and principles into their data processing activities, such as by conducting privacy impact assessments and appointing privacy officers.

Increasing clarity and simplicity for entities and individuals

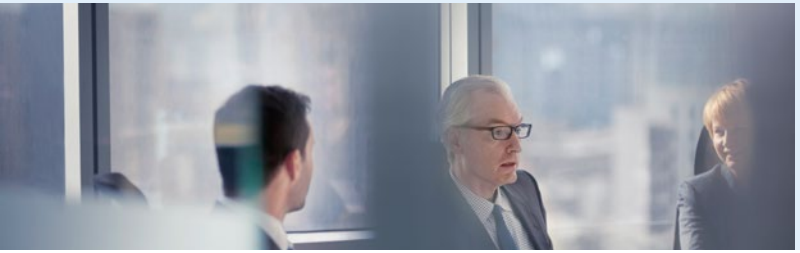
The Government recognises in its report that businesses need a clear and consistent framework to comply with their privacy obligations and to facilitate innovation and growth in the digital economy. To this end, the Government has committed to amend the Privacy Act to provide 'clarity and simplicity' for regulated entities, such as by simplifying some of the APPs, clarifying the scope and application of the Act, and harmonising the privacy regime with other jurisdictions and international standards. By providing more certainty and flexibility, the Government aims to empower businesses to take advantage of the '*opportunities presented by emerging technologies*', such as AI and big data, whilst ensuring that they respect and protect the privacy of individuals.

Improving control and transparency for individuals over their personal information

The Government has endorsed in-principle the ability of individuals to seek redress for interferences with their privacy, either through the OAIC or directly through the courts. Currently, individuals can only make a complaint to the OAIC, which has limited powers to resolve disputes and impose sanctions. **The Government has agreed to explore the following options to augment the rights of individuals**:

- a direct right of action that would allow individuals to bring civil proceedings against an entity for breaches of the Privacy Act, without having to lodge a complaint with the OAIC first. This would enable individuals to seek remedies such as injunctions, declarations, damages, or apologies from the entity directly responsible for the breach; and
- a statutory tort for serious invasions of privacy that would create a new civil cause of action for individuals who suffer harm or distress as a result of an intentional or reckless interference with their privacy that is not covered by the Privacy Act. This could include scenarios such as surveillance, disclosure of sensitive information, or misuse of personal data.

Although the Government acknowledged in its report the potential costs and risks associated with these proposals (such as increased litigation, insurance premiums and compliance burden), following the 'doxing' of more than 600 individuals from a WhatsApp group in February, the Government has signaled that it may bring these aspects forward.



> By providing more certainty and flexibility, the Government aims to empower businesses to take advantage of the '*opportunities presented by emerging technologies*', such as AI and big data, whilst ensuring that they respect and protect the privacy of individuals.

Strengthening enforcement

The Government has agreed to a range of proposals designed to increase the enforcement capabilities of the OAIC. This includes:

- conducting a strategic review of the OAIC's resourcing, structure, and powers, to ensure that it can respond to the evolving privacy landscape and the increasing volume and complexity of privacy complaints and breaches;
- introducing an additional new category of civil penalty provisions to capture administrative breaches of the Privacy Act;
- providing the OAIC with new powers to issue assessment notices to require entities to demonstrate their compliance with the Privacy Act; and
- requiring the OAIC to maintain a register of privacy codes and code members, and to publish information about its enforcement activities.

These changes are in addition to the significant increase in the maximum civil penalties for serious and/or repeated interferences with privacy that were enacted in December 2022 - which increased penalties from $2.2 million to an amount not more than the greater of:

- $50 million; or
- if a court can determine the value of the benefit that the body corporate (and its related bodies corporate) directly or indirectly obtained from the contravention – three times the value of that benefit; or
- if a court cannot determine the value of that benefit – 30% of the adjusted turnover of the body corporate during the breach turnover period (minimum 12 months) for the contravention.

Next steps

In addition to the doxing-related legislation discussed above, for those proposals that are agreed by the Government, we anticipate that draft amending legislation will be released for comment at some stage this year. For those that are agreed in-principle, the Government will continue consultation, with a view to appropriately balancing privacy protections with economic impacts and the increased regulatory burden on organisations.

A more detailed description of the Government's response to the AG Report can be found in our article, The long road to Australian privacy reform.

4.2 Security of Critical Infrastructure laws

On 22 November 2023, the Federal Government released its 2023-2030 Cyber Security Strategy, which sets out further proposed changes to the Security of Critical Infrastructure Act (2018) (**SOCI Act**).

Protection of critical data in 'business critical' data storage systems

As discussed in section 3.1, to address the increasing number of cyber incidents involving non-personal data (such as financial information and valuable IP), it is proposed that the definition of 'asset' will be amended to include data storage systems that hold 'business critical data'.

'Last resort' consequence management power

The Strategy proposes the introduction of a 'last resort' power that would allow the Minister for Home Affairs to intervene directly in the operations of a critical infrastructure entity in the event of a serious cyber incident. This power would only be used as a last resort, when the Minister is satisfied that there is an imminent and serious threat to Australia's national security, defence or socio-economic stability, and that the entity is unable or unwilling to take appropriate action to mitigate the threat. The Minister would be able to issue directions to the entity or its staff, or authorise the Australian Cyber Security Centre (**ACSC**) to access or take control of the entity's systems, data or premises. The Minister would also be required to consult with the relevant state or territory minister and the affected entity before exercising this power, and to report to Parliament on its use within six months.

The purpose of this power is to enable the Government to address the aftermath of a serious cyber incident experienced by a critical infrastructure entity, and in so doing, protect the public interest and national security.

Simplification of information sharing between government and industry stakeholders

Controlled information sharing is a key aspect of ensuring the security and resilience of critical infrastructure. The Government is concerned that the current framework regulating the disclosure and use of 'protected information' by critical infrastructure entities to government may be overly complex and restrictive, creating barriers to effective collaboration and risk management. To address this issue, two amendments have been proposed to the SOCI Act, to simplify and clarify the information sharing regime:

- owners or operators of critical infrastructure assets would be permitted to disclose protected information to owners or operators of other critical infrastructure assets, Commonwealth regulators or relevant third parties, for the purpose of mitigating or responding to a cyber incident, a serious physical incident, or an adverse operational event affecting their services. This would enable coordinated action to prevent or minimise the impact of such incidents on critical infrastructure and the broader public interest; and
- critical infrastructure entities would be permitted to disclose protected information to all Commonwealth, state and territory government entities where disclosure is necessary for the purpose of upholding the security or resilience of critical infrastructure or protecting national security or socio-economic stability.

Review and remedy powers

The Secretary for Home Affairs (or a relevant Commonwealth regulator) would have the authority to issue formal, written directions to critical infrastructure entities in certain situations. These would require relevant entities to take specific actions to address gaps or weaknesses in their critical infrastructure risk management programs. This directions power would only be exercised as a last resort, when the cooperation of the entity is insufficient or ineffective, where the deficiency carries a material risk, and poses a severe and credible threat to socio-economic stability, defence or Australia's national security.

Consolidation of telecommunication security requirements

A key objective of these further SOCI Act reforms is to harmonise the cyber security obligations for critical infrastructure entities across different sectors and reduce regulatory duplication. To this end, the Government proposes to move the security requirements for telecommunication providers from Part 14 of the *Telecommunications Act 1997* (Cth) to the SOCI Act and align those requirements with the SOCI Act's enhanced positive security obligations under a new 'Telecommunications Security and Risk Management Program' (**TSRMP**). The TSRPM will cover both the physical and cyber security aspects of protecting telecommunication networks and services from malicious interference, unauthorised access or damage.

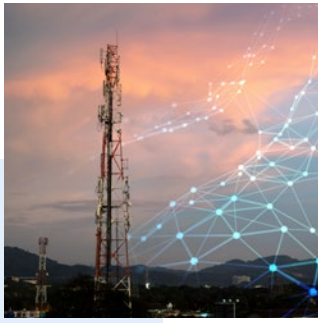
We provide a detailed analysis of the these proposed SOCI Act reforms in our recent publication, Australia's evolving cyber security landscape: Consultation launched.

CISC's changing compliance regulatory posture

On 6 March 2024, the Cyber and Infrastructure Security Centre (CISC) announced changes to its compliance regulatory posture for the SOCI Act. The compliance focus for 2023-2024 was on education and awareness raising, except for any detected egregious non-compliance.

During the third and fourth quarters of 2023-2024 CISC intends to undertake a limited series of trial audits which will test industry compliance with SOCI Act obligations. The outcome of these trials will inform and guide the commencement of compliance audit activities in 2024-2025. In 2024-25, CISC will aim to balance education and awareness raising activities with compliance activities to drive an uplift in regulated entity compliance.

This shift in CISC's enforcement strategy is clearly designed to ensure there is a continuing focus by regulated entities on understanding the implications of their SOCI Act obligations and acting to protect the critical infrastructure and essential services on which Australians rely.



4.3 Further cyber security legislative reforms

The Strategy proposes four additional legislative reforms.

Secure-by-design standards for IoT devices

This Strategy proposes a mandatory cyber security standard for consumer-grade IoT devices. More specifically, in order to align with international standards, the Government proposes to adopt the first three principles of the ETSI EN 303 645 standard which mandates cyber security for relevant IoT devices in the Australian market. These principles are:

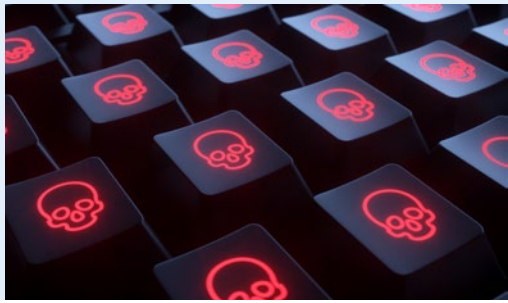
- no universal default passwords – IoT devices should not have any passwords that are shared across multiple devices or that are easy to guess;
- vulnerability reporting policy – IoT device manufacturers must have a policy that allows security researchers or other parties to report any vulnerabilities they find in the devices and must continually monitor for and address security vulnerabilities with their devices; and
- keep software updated – IoT devices should support secure and timely software updates, and IoT device manufacturers must ensure that updates do not compromise the security of the device and that the integrity of updates is verified.

Ransomware reporting obligations

After much debate on the various approaches to combat the growing threat of ransomware attacks, the Government proposes to implement no-fault, no-liability mandatory reporting obligations for ransomware incidents. Two reporting obligations are proposed:

- firstly, an entity that receives a demand from an attacker to pay a ransom (for example, in exchange for restoring access to encrypted data or preventing the public release of their data) must report to the Government that it has the subject of such an attack and provide details of the attacker, the amount and form of payment demanded, and the impact of the attack on the entity's operations and data; and
- a second reporting obligation would apply where the entity decides to make a payment to the attacker, either in response to the initial demand or after further negotiations. The entity would have to report to the Government that it has made such a payment and provide details of the amount and form of payment, the identity and location of the recipient, and the outcome of the payment (for example, whether the data was decrypted or released).

The Government has not yet specified the timeframe or mechanism for making these reports, but has indicated that it intends to make the reporting process as simple and streamlined as possible, and that it will provide guidance and assistance to the reporting entities. In relation to the 'no fault' aspect of the regime, the Government will not impose any penalties or sanctions on the reporting entities – although it has equally stated **that making a ransomware report would not excuse reporting entities from their existing regulatory obligations**. This means that an entity could still be held liable for a failure to comply with its security-related obligations under APP 11, the SOCI Act or other applicable laws, or pursuant to contractual obligations that it owes to third parties.



Limited-use obligation for utilisation by the Australian Signals Directorate and the National Cyber Security Coordinator

A key challenge in responding to ransomware attacks is the lack of information sharing and collaboration between the affected entities and government agencies. The Government has proposed a limited-use obligation to encourage reporting entities to share cyber incident information with the Australian Signals Directorate (**ASD**) and National Cyber Security Coordinator (**Cyber Security Coordinator**), without fear of regulatory reprisal. The information reported under this obligation would be used only for the purposes of assisting reporting entities to manage the consequences of an attack, such as restoring their systems, recovering their data, and preventing further harm. Importantly, the information would not be used to initiate or support any investigation or enforcement action against the reporting entity, nor would it be disclosed to any third parties without the entity's consent. The intention here is to create a 'safe space' for information sharing and foster a collaborative approach to addressing ransomware threats.

Cyber Incident Review Board

The Government's final legislative proposal seeks to improve the collective understanding and awareness of cyber incidents and their impact on Australia's economy, security and society at large. To this end, the Government proposes to establish a Cyber Incident Review Board (**CIRB**) that would conduct independent and impartial reviews of 'significant' cyber incidents affecting reporting entities. The CIRB would not have any enforcement, intelligence or regulatory powers or functions, but would rather act as a learning and improvement mechanism. The CIRB would examine the causes, consequences and responses to cyber incidents, and make recommendations on how to prevent, mitigate and recover from future incidents. The CIRB will also publish de-identified and anonymised reports of its findings and recommendations to enhance public awareness and improve overall cyber resilience.

A more detailed description of the these proposed legislative reforms is set out in our recent publication Australia's evolving cyber security landscape: Consultation launched.

4.4 Digital and identification developments

On 30 November 2023, the Federal Government introduced the *Digital ID Bill 2023* (Cth) (**Digital ID Bill**) into Parliament. Most recently, the Senate Economics Legislation Committee has completed its inquiry of the Digital ID Bill, and issued a report on 28 February 2024. The Digital ID Bill aims to provide individuals with secure, convenient, voluntary and inclusive ways to verify their identity for use in online transactions with government and business. The Digital ID Bill aims to:

- legislate and strengthen a voluntary Accreditation Scheme for digital ID service providers that wish to demonstrate compliance with best practice privacy, security, proofing and authentication standards;
- legislate and enable expansion of the Australian Government Digital ID System (**AGDIS**) for use by the Commonwealth, State and Territory governments, and eventually private sector organisations;
- embed strong privacy and consumer safeguards (in addition to those under the Privacy Act) to ensure users are protected; and
- strengthen governance arrangements for the Accreditation Scheme and the AGDIS, including by establishing the Australian Competition and Consumer Commission (**ACCC**) as the Digital ID Regulator, and expanding the role of the OAIC to regulate privacy protections for digital IDs. Both of these regulators will have a broad range of powers under the Digital ID Bill, including to impose civil penalties.

The Digital ID Bill also proposes a series of enhanced privacy obligations for participants, including:

- data breach notification obligations – which are in addition to the existing notification requirements under the Privacy Act, and may require notification of any 'cyber security incident' to the Digital ID Regulator;
- an extension of the definition of 'personal information' to include 'attributes' used by the accredited provider that are not otherwise covered by the Privacy Act definition; and
- the introduction of a number of new privacy related obligations (in addition to those already set out in the Privacy Act) that apply to all accredited entities.

The Digital ID Bill is a key component of the Government's broader agenda to modernise digital identification systems across public sector service platforms, and to enhance the security and privacy of individuals' sensitive and other personal data in light of increasing cyber threats.

"

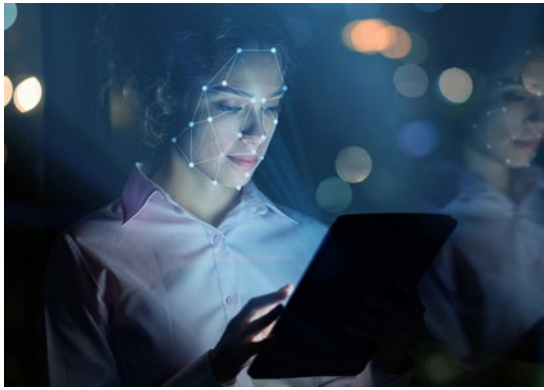
The Digital ID Bill is a key component of the Government's broader agenda to modernise digital identification systems across public sector service platforms, and to enhance the security and privacy of individuals' sensitive and other personal data in light of increasing cyber threats.

Another component of this agenda is the Government's introduction, in September 2023, of the *Identification Verification Services Bill 2023 (Cth)*, which was passed by both Houses in December 2023. The *Identification Verification Services Act 2023 (Cth)* (**Identification Verification Services Act**) came into effect on 15 December 2023, and reflects the Government's increased focus on digital verification and its broader interest in boosting the digital economy through regulatory development. In part, this Act was introduced to address the cyber risks associated with disparate entities each having to collect and hold identification information (such as driver's licences and passport details), and instead seeks to implement a more centralised process. Under the Identification Verification Services Act, the Attorney-General's Department is authorised to develop, operate and maintain three identity verification facilities:

- **Document verification service (DVS Hub)** – the DVS hub allows a requesting party to verify with the Government whether the biographic information on an individual's identity document matches the original record.
- **Face Matching Service Hub** – this is an identity verification service that uses facial recognition technology to compare the biometric information of an individual with one or more sources of identification documents. The service has two main functions:
  - a one-to-one matching service that allows a requesting party, such as a bank or an airline, to verify that an individual's face matches the photo on their Commonwealth, state or territory issued identification document (such as a passport or a driver's licence); and
  - a one-to-many matching service that allows a requesting authority, such as a law enforcement agency or an intelligence organisation, to identify a person of interest by matching their face against a pool of facial images from multiple identification documents. However, this function is limited to verification of 'shielded persons', being individuals whose identity or safety may be at risk due to their involvement in a criminal investigation, witness protection program or domestic violence situation. The shielded persons' facial images are encrypted and stored separately from the other facial images, and can only be accessed by authorised requesting authorities under strict conditions.
- **National Driver Licence Facial Recognition Solution (NDLFRS)** – the NDLFRS enables the verification of a person's identity by comparing their facial image against a database of driver's licence and other identification photos held by state and territory authorities. The system can perform a one-to-one match to prevent identity fraud and enhance security for various transactions and services that require proof of identity.

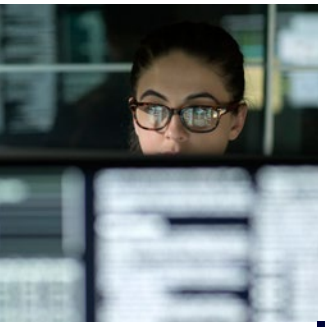
Organisations that wish to access these identity verification facilities can do so by entering into two types of agreements that govern the requesting and provision of the identity verification services:

- **participation agreement** – an agreement between the Attorney-General's Department and other authorities, persons and bodies about the requesting and provision of identity verification services using the approved identity verification facilities; and
- **NDLFRS hosting agreement** – an agreement between the Attorney-General's Department and authorities of a state or territory that supply identification information stored and used in the NDLFRS.



4.5 Regulator action

In response to the increasing frequency and severity of data breaches affecting millions of Australians, the OAIC has adopted a more stringent and proactive stance in its enforcement of the Privacy Act. In particular, the OAIC has been taking a more robust approach in its assessment of whether eligible data breaches have been notified in a timely manner, as demonstrated by the following recent cases.



Australian Information Commissioner v Australian Clinical Labs

The OAIC launched its second ever civil penalty action in the Federal Court against Australian Clinical Labs (**ACL**), following a data breach in February 2022 affecting millions of Australians. The first civil penalty action, against Meta relating to the Cambridge Analytica scandal, is ongoing.

The OAIC alleges that ACL failed to assess and notify the breach in a timely manner as required under the Privacy Act. It also asserts that from May 2021 to September 2022, ACL seriously interfered with the privacy of millions of Australians by failing to take reasonable steps to protect their personal information from unauthorised access or disclosure (in breach of the Privacy Act) which further left the organisation vulnerable to cyber attack.

Pacific Lutheran College and *Datateks*

Two decisions of the Australian Information Commissioner handed down in October 2023, *Pacific Lutheran College (Privacy)* [2023] AICmr 98 and *Datateks Pty Ltd* [2023] AICmr 97, highlight the importance of an organisation assuming that a data breach has occurred even when it is not possible to conclusively determine that personal information has been exfiltrated. In each of these cases, the OAIC found that the organisations had breached their obligations under the Privacy Act by failing to conduct an adequate assessment of a suspected data breach within 30 days and notifying an eligible data breach to the OAIC and affected individuals as soon as practicable.

Importantly, the OAIC emphasised that where there is doubt or uncertainty about whether personal information has been compromised, the organisation should err on the side of caution and take steps to protect the privacy of potentially affected individuals. The OAIC also found that the organisations did not have effective policies and procedures in place to respond to data breaches in a timely and comprehensive manner, and imposed various remedial actions on them, including preparing and implementing incident response plans. These decisions demonstrate that the OAIC expects organisations to take a proactive, pre-emptive and timely approach to data breach management, and that failure to do so may result in regulatory action. The regulatory stakes will be higher still should the OAIC gain additional powers to impose graduated civil penalties, as discussed in section 4.1.

> These decisions demonstrate that the OAIC expects organisations to take a proactive, pre-emptive and timely approach to data breach management, and that failure to do so may result in regulatory action.

4.6 Increased funding for the OAIC

The 2023-24 Federal Budget announced significant additional funding for the OAIC. Specifically, over four years, the OAIC will receive $44.3 million (of which $17.8 million will be received for the 2023-24 financial year). The additional funding is intended to support privacy enhancing activities generally, and includes the reinstatement of the three-Commissioner model – the Australian Information Commissioner (as agency head), the Privacy Commissioner, and the Freedom of Information Commissioner.

4.7 Data breach class action updates

In the aftermath of the data breaches that affected Medibank and Optus customers, several class actions have been initiated against the two organisations. These class actions variously seek compensation for alleged breaches of privacy, negligence, consumer law and corporations law, as well as for the potential harm caused by the unauthorised disclosure of personal and sensitive information.

Seven different firms – Baker McKenzie, Maurice Blackburn, Slater and Gordon, Phi Finney McDonald, Quinn Emanuel and Omni Bridgeway / Balance Legal Capital (as litigation co-funders) – are considering, or have launched, class actions against Medibank.

Two different firms - Slater and Gordon and Maurice Blackburn - have respectively launched a class action and a representative complaint against Optus.

The commenced actions against Medibank and Optus are currently ongoing.

4.8 Growing activity amongst other Australian regulators

As cybercrime affects ever greater numbers of Australian organisations and individuals, other regulators besides the OAIC have strengthened efforts to promote better data management practices and to mitigate the harms caused by malicious third party actors. Not all of these regulatory actions have led to enforceable outcomes; however, there is a shared understanding amongst Australian regulators that enhancing cyber resilience is vital for Australia's long term socio-economic stability and national security.

> "there is a shared understanding amongst Australian regulators that enhancing cyber resilience is vital for Australia's long term socio-economic stability and national security."

4.9 Australian Competition and Consumer Commission (ACCC)

The ACCC has continued to demonstrate active interest in the intersection between competition and consumer law, on the one hand, and the protection of personal information on the other. This intersection is not new, as evidenced by the Consumer Data Rights (**CDR**) regime established under the *Competition and Consumer Act 2010* (Cth), which aims to give consumers greater control over their data. However, the ACCC has intensified its scrutiny of data handling practices by Australian organisations this past year, in response to the growing risks and challenges posed by the digital economy.

- ***ACCC v Meta***: On 26 July 2023, in *ACCC v Meta Platforms Inc*, the Federal Court imposed a $20 million pecuniary penalty on Meta's subsidiaries, Facebook Israel and Onovo Inc. The Court held that the subsidiaries had breached Australian Consumer Law by misleading users about the way those companies used customer data within the 'Onavo Protect app', a free VPN service that did not adequately disclose that certain data would be used for other commercial purposes.
- **Digital Platform Services Inquiry (Issues Paper)**: In collaboration with the OAIC, the ACCC welcomed the opportunity for submissions to be posted in its issues paper titled 'Digital Platform Services Inquiry – March 2024 report on data brokers' dated 10 July 2023. The issues paper draws upon the privacy law framework in its consideration of whether regulatory reforms are required to address consumer protection issues in the data-handling practices of third party data brokers.
- **Collaborative enforcement and monitoring of CDR**: In October 2023, the ACCC and OAIC released an updated version of the Compliance and Enforcement Policy for the Consumer Data Right. The policy highlights the approach adopted by both regulators in their combined monitoring of CDR compliance. Importantly, in undertaking enforcement action against potential breaches of the CDR regime, the regulators may consult with each other and coordinate action (although they can still exercise their own discretion to take separate enforcement action, if required).

"The ACCC has intensified its scrutiny of data handling practices by Australian organisations this past year, in response to the growing risks and challenges posed by the digital economy."

4.10 Australian Securities and Investments Commission (ASIC)

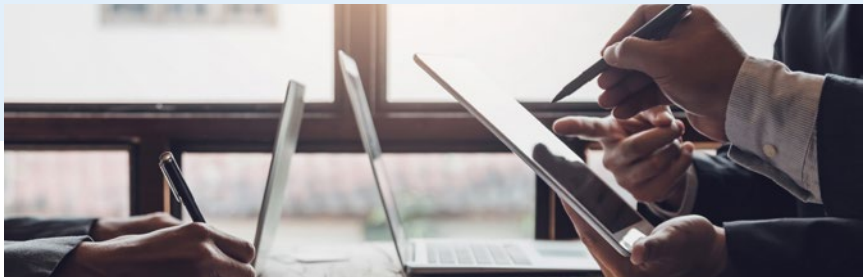
ASIC's Chair, Joe Longo, has urged Australian organisations to make cyber security and resilience a top priority. In this section, we summarise some of the recent initiatives and developments that ASIC has undertaken or announced in relation to cyber security.

- **Cyber Pulse Survey findings**: ASIC released its Cyber Pulse Survey 2023 findings in November 2023. The survey aims to assess the cyber maturity of organisations regulated by ASIC. The survey revealed that most organisations took a reactive approach to managing their cyber security framework, rather than a proactive one that anticipates and prevents potential threats. The survey also identified several areas where organisations could improve their cyber resilience, such as managing risks from third party suppliers, protecting data from unauthorised access or loss, planning for crisis response and recovery, and aligning with best practice cyber security standards.

- **Directors' duties**: ASIC continues to reinforce the notion that prioritising cyber security and resilience is necessary for avoiding a breach of directors' duties. In ensuring directors are discharging their duties effectively, an organisation's risk management framework must adequately address cyber security risks.

  Amongst other considerations, active oversight of third party cyber risks within supply chains should form part of a board's evaluation of cyber risk. This includes ensuring the organisation has robust contracts with key suppliers that set out expectations and obligations around cyber security, as well as mechanisms to monitor and audit their performance. These obligations are also consistent with new APRA requirements under CPS 230 (discussed in section 4.11).

Furthermore, on 28 February 2024, the Australian Institute of Company Directors (**AICD**), in collaboration with the Cyber Security Cooperative Research Centre (**CSCRC**), released its framework titled Governing Through a Cyber Crisis (**AICD Framework**) which provides comprehensive guidance to assist directors in both preparing for and responding to cyber crises. Central to the AICD Framework is the expectation that directors have a deep understanding of their internal infrastructure (such as networks, digital assets and policies) to mitigate cyber risks. The AICD Framework provides ASIC with a benchmark for determining whether directors have discharged their duties through adopting appropriate risk management and governance practices.



4.11 Australian Prudential Regulation Authority (APRA)

Recognising the heightened threat of cyber attacks and their potentially devastating impact on the stability of the financial system, APRA has been proactively regulating the cyber security practices of entities under its supervision. **APRA-regulated entities, which hold substantial amounts of financial and personal data vital to the economic well-being of Australians, are expected to demonstrate a high level of cyber resilience and preparedness**. The following section outlines some of the recent developments and initiatives that APRA has undertaken to enhance its cyber security oversight and guidance.

- **Audit of CPS 234 compliance:** A key measure introduced by APRA to enhance the cyber security posture of its regulated entities was Prudential Standard CPS 234 (Information Security) which came into effect on 1 July 2019 (and 1 July 2020, or the next contract renewal date with the relevant third party if earlier, for obligations related to information assets managed by third parties). CPS 234 sets out certain minimum requirements for information security management, including identifying and protecting information assets, detecting and responding to cyber incidents, and testing and auditing information security capabilities.

  To ensure compliance with this standard, APRA has required its regulated entities to conduct one-off tripartite assessments by an independent auditor, which has involved verifying the implementation of the standard's requirements, assessing the effectiveness of the controls in place, and reporting any material weaknesses or gaps to APRA.

  The results of these assessments have revealed that, while most entities had made significant progress in aligning their information security practices with the standard, there are still several areas for improvement. These include:

  - **inadequate labelling of critical and sensitive information assets** – some entities did not have a clear and consistent classification scheme for their information assets, which made it difficult to determine the appropriate level of protection and access control for each asset. This could expose entities to the risk of unauthorised access, disclosure or modification, or loss of information assets, particularly in the context of outsourcing or third party arrangements;
  - **deficient incident response plans** – some entities did not have comprehensive and tested plans for responding to cyber incidents, which could affect their ability to contain, mitigate and recover from a cyber incident, as well as communicate with relevant stakeholders and regulators; and
  - **lack of regular testing and assurance activities** – some entities did not conduct sufficient testing and assurance activities to validate the effectiveness of their information security controls and identify any potential vulnerabilities or gaps.

  APRA expects all regulated entities to address the findings of their tripartite assessment and remediate any non-compliance issues as soon as possible.

- **Finalised CPS 230**: On 17 July 2023, APRA released the final version of Prudential Standard CPS 230 (Operational Risk Management). CPS 230, which is intended to complement CPS 234, sets out expected standards for APRA regulated entities to manage operational risk, as well as specific requirements relating to business continuity and service provider management. **CPS 230 takes effect on 1 July 2025, and APRA expects full compliance by this date**. A more detailed summary of CPS 230 can be found in our article CPS 230: Your roadmap to compliance.

5

Significant Australian and international data breaches

5. Significant Australian and international data breaches

The past 12 months have seen severe and widespread data breaches in Australia and around the world, with the health and finance sectors particularly impacted.

5.1 Significant data breaches

In the last 12 months, data breaches greatly increased in frequency and scale, driven predominantly by malicious or criminal activity.

Between July to December 2023, malicious or criminal activity comprised 67% of all notifications to the OAIC (322 incidents, up 12% from 287 in the first half of 2023). In terms of all reported data breaches (including those resulting from malicious or criminal attacks, human errors and system faults), the health and finance sectors remained the top reporters. The health sector reported 104 breaches (22% of all notifications) while the finance sector reported 49 breaches (10% of all notifications). The majority of breaches (65%) affected 100 or fewer people. Furthermore, 121 secondary notifications were reported, which was a significant increase from the 29 secondary notifications reported in the first half of 2023.

This increase in malicious and criminal activity is also reflected in the ASD's Cyber Threat Report 2022-23, which states that 94,000 cybercrime reports were made to law enforcement through ReportCyber in 2022-23, an increase of 23% as against the previous year.

Some of the more significant cyber breaches, both in Australia and internationally, that captured public attention over the last 12 months, and which demonstrate the potential impact of cyber threats on organisations across every sector, are set out below.

> In the last 12 months, data breaches greatly increased in frequency and scale, driven predominantly by malicious or criminal activity.

From July to December 2023

483

incidents were reported to the OAIC (**+19% in 6 months**)

22%

of these notifications reported by the Health sector

10%

of these notifications reported by the Finance sector

5.2 Significant Australian data breaches

Entity	Date	Threat actor	Magnitude of impact	Affected information
Tangerine	February 2024	Hackers	Over 200,000 customers	Personal information of customers, including full names, dates of birth, email and postal addresses and mobile phone numbers
Australian Human Resources Institute	February 2024	Hackers	Unknown	TBC
Football Australia	February 2024 (ongoing leak traced since 2022)	Not confirmed - likely human error	Unknown	Personal information of football players and ticket purchasers
Elite Supplements	January 2024	Hackers	Unknown	Personal information of online customers, including full names, shipping and email addresses and phone numbers
Hal Leonard Australia	January 2024	Ransomware group known as Qilin ransomware gang	37.6 GB of data	Private contracts, financial documentation, email correspondence and project information
Court Services Australia	January 2024	Ransomware group known as Qilin ransomware gang	Unknown	Court recordings database, including audio-visual recordings of court hearings and transcription services
Nissan Australia	December 2023	Ransomware group known as Akira	100 GB of data	Sensitive business and client data
Yakult Australia and New Zealand	December 2023	Hackers group known as DragonForce	95 GB of data	Sensitive employee information including scans of passports and drivers' licences, pre-employment medical assessments and certificates, salaries, and performance reviews
St Vincent's Health	December 2023	Hackers	Unknown	TBC
Duolingo	November 2023	Hackers	2.6 million users	Personal information of users, including email addresses, usernames, names and phone numbers, information about social networks and other generic information such as language studies, experience, progress and achievements
DP World	November 2023	Hackers	Unknown	Personal details of employees
Dymocks	October 2023	Hackers	1 million customers	Customer names, email addresses and mobile numbers
Tissupath	September 2023	Hackers	Unknown	Customer records from 2011 to 2020 specific to pathology referrals for suspected cancer patients
Pizza Hut	September 2023	Hacking group known as ShinyHunters	193,000 customers	Customer names, delivery addresses, emails and phone numbers
HWL Ebsworth	April 2023	Hacking group known as ALPHV/ Blackcat	2.5 million files	Sensitive information relating to government department and agencies

5.3 Significant international data breaches

Entity	Country	Date	Threat actor	Magnitude of impact	Affected information
Trello	Global	January 2024	Hackers	Over 15 million records	Full names and email addresses of users
Adobe, LinkedIn and Twitter (and others) collectively	Global	January 2024 (discovery of leak)	TBC	26 billion records	TBC
AnyDesk	Global	January 2024	Hackers	TBC	Source code and code signing certificates
Dori Media Group	Israel	December 2023	Hacking group known as MalekTeam	Over 100 TB of data	TBC
Real Estate Wealth Network	USA	December 2023	Hackers	1.5 billion records	Property history, motivated sellers, bankruptcy information, divorce, tax liens, foreclosure, home owner association liens, inheritance, court judgments, obituary, vacant properties and more
Bank of America & Infosys	USA	November 2023	Ransomware group known as LockBit	Over 57,000 customers	Home addresses, full names, dates of birth, social security numbers and other forms of financial information
Boeing	Global	November 2023	Ransomware group known as LockBit	Approximately 45 GB of data	Sensitive data records
Okta	USA	October 2023	Hackers	Unknown	Full names and email address
23andMe	USA	October 2023	Hackers	7 million users	Genetic data profiles
ICMR Indian Council of Medical Research	India	October 2023	Hackers	815 million users	Name, age, gender, address, passport number and Aadhaar number (a 12-digit government identification number
MOVEit	USA	September 2023	Ransomware group known as Cl0p	Over 60 million users	Corporate and personal data
Darkbeam	UK	September 2023	Employee error	Over 3.8 billion records	Data records
UK Electoral Commission	UK	August 2023	Hackers	40 million voters	Names, addresses, dates on which individuals achieve voting age, telephone numbers and email addresses
Tigo	Hong Kong	July 2023	Data leak	146 million records	Names, usernames, genders, email addresses and IP addresses
MCNA Insurance	USA	May 2023	Ransomware attack	Over 8.9 million individuals	Names, addresses, dates of birth, phone numbers, email addresses, social security numbers, driver's licence numbers and other government-issued ID details
PharMerica	USA	May 2023	Ransomware attack	5.8 million patients	Names, addresses, dates of birth, social security numbers, health insurance data and medical data belonging to alive and deceased individuals

6

Ten lessons for best practice cyber response

6. Ten lessons for best practice cyber response

Over many years of advising on data breaches, we've seen first-hand the consequences of underinvesting in cyber security, as well as the benefits of taking proactive measures to prevent and mitigate serious cyber incidents.

Here are our ten key lessons for best practice cyber response.

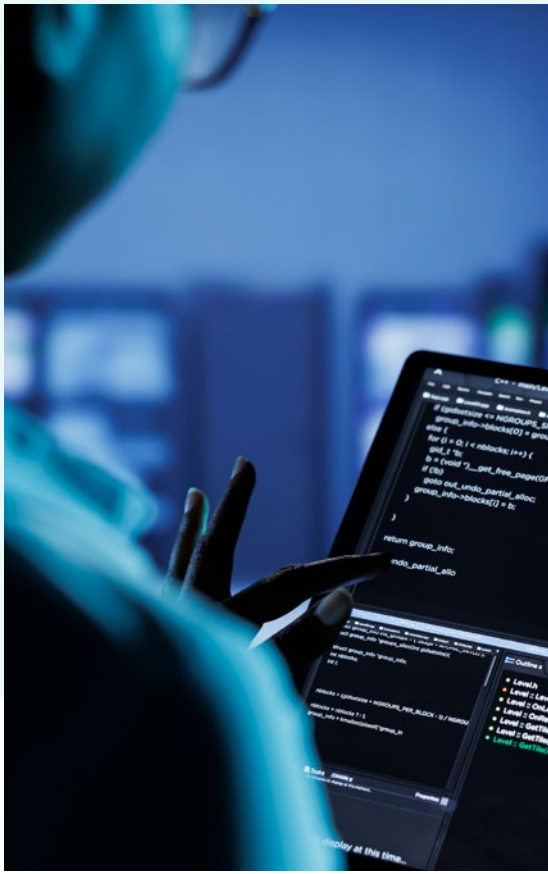
LESSON 1 ›

Don't underinvest in cyber

Underinvesting in cyber security can result in financial losses, reputational damage, legal jeopardy, and operational disruption. **It is crucial for companies to prioritise cyber security as a strategic investment to protect their assets, customers and overall business interests**. By making prudent investments in cyber security, organisations can achieve early incident detection (or avoid an incident entirely), mitigating the impact of a breach.

Investing in cyber security involves proactively dedicating resources to protect digital assets and data from cyber threats. This proactive approach broadly involves hiring cyber security experts; implementing robust security governance, policies and procedures; deploying protective technologies and tools; educating employees; safeguarding data through encryption and access controls; planning and preparing for incident response and recovery; adhering to regulatory requirements; monitoring for threats; and managing third and fourth party (supply chain) risks. It requires an ongoing commitment to adapt and allocate budget to address an ever-changing cyber risk landscape.

NotPetya provides a compelling example of why underinvesting in cybersecurity may be detrimental to an organisation. This destructive malware had a global impact, highlighting the potential devastation of a single cyberattack. It exposed vulnerabilities in supply chains, resulting in financial losses, reputational damage and regulatory consequences. NotPetya also emphasised the need for robust crisis preparedness and global collaboration. Find out more in the fascinating article 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History'.



LESSON 2 ›

This is more serious than ever

Cyber breaches are instigated by diverse threat actors, including cyber criminals driven by financial motives, nation-state actors engaged in espionage and disruptive cyber attacks, hacktivists promoting social or political agendas, organised crime groups seeking financial gains, 'script kiddies' causing disruptions for notoriety, advanced persistent threat (**APT**) groups conducting targeted cyber espionage, and rogue insiders misusing their access. Additionally, third (or fourth) party vendors can inadvertently introduce vulnerabilities into the supply chain. Given this multifaceted threat landscape, organisations must maintain constant vigilance and robust cyber security defences to protect against the range of threat actors and their evolving strategies and tactics.

Human error is the cause of around 95% of cyber incidents, underscoring the need for organisations to prioritise a privacy- and security-by-design approach.

This involves integrating robust security and privacy practices throughout an organisation's operations, and anticipating and mitigating human-related risks. Key measures include employee training, access controls, regular audits, incident response plans, secure development practices, data encryption, and continuous improvement efforts. By proactively anticipating and addressing human errors and vulnerabilities, organisations can enhance their cyber security resilience and reduce the occurrence and impact of cyber incidents.

Regulators around the world (and in Australia, ASIC, APRA, OAIC and ACCC) are taking an increasingly aggressive enforcement approach to privacy and data protection incidents. This is driven by the growing recognition of the dangers posed by sophisticated malicious actors to the economy and to national security – underlining the need for organisations to play their part in safeguarding their data, the privacy of their customers, and their critical infrastructure.

LESSON 3 ›

Have a plan

In the critical first 24-48 hours of responding to a ransomware or other cyber attack, maintaining a calm and rational approach is essential because panic tends to lead to poor decision-making. Ransomware is a particularly challenging problem, often referred to as a 'wicked problem' due to its ever-evolving and complex nature. **Unaided human judgment can be flawed, influenced by vivid events, optimism bias, and cognitive narrowing under pressure**. To counter these tendencies, formal analytical techniques, along with regular training exercises and discussions, provide invaluable tools to navigate the challenges posed by ransomware and other cyber attacks.

Having a comprehensive and well-tested incident response plan is indispensable during a cyber attack (as well as being a regulatory expectation, as discussed in section 4), as it enables organisations to respond promptly and effectively. It aids in minimising damage by swiftly identifying the extent of the attack, containing it, and

facilitating communication with relevant parties. This plan assists in complying with regulatory requirements, guides recovery efforts, manages risk, fosters consistency, and enhances employee preparedness. Additionally, it offers a mechanism for continuous improvement, by evaluating and adjusting response strategies from prior learnings.

Staff awareness and training programs are also a critical aspect of organisational cyber resilience, and assist in both data protection and regulatory compliance. A well-trained workforce can enhance public trust and the organisation's reputation, making them key components of an organisation's broader cyber security strategy.

LESSON 4 ›

Bring in third party experts to assist you at an early stage

Engaging third party experts in the early stages of cyber attack preparedness provides organisations with specialised knowledge, objectivity, and experience.

Conversely, relying solely on an internal team during a crisis may introduce the challenge of proximity bias, where their closeness to the situation could hinder the ability to make objective and impartial decisions. Additionally, IT staff, whilst skilled in various technical aspects, typically lack specialised expertise in security and incident response. As a result, **organisations often benefit from engaging external experts who can bring a fresh perspective, in-depth security knowledge, and a dispassionate approach to resolving incidents swiftly and effectively**.

LESSON 5 ›

Don't engage in 'blamestorming'

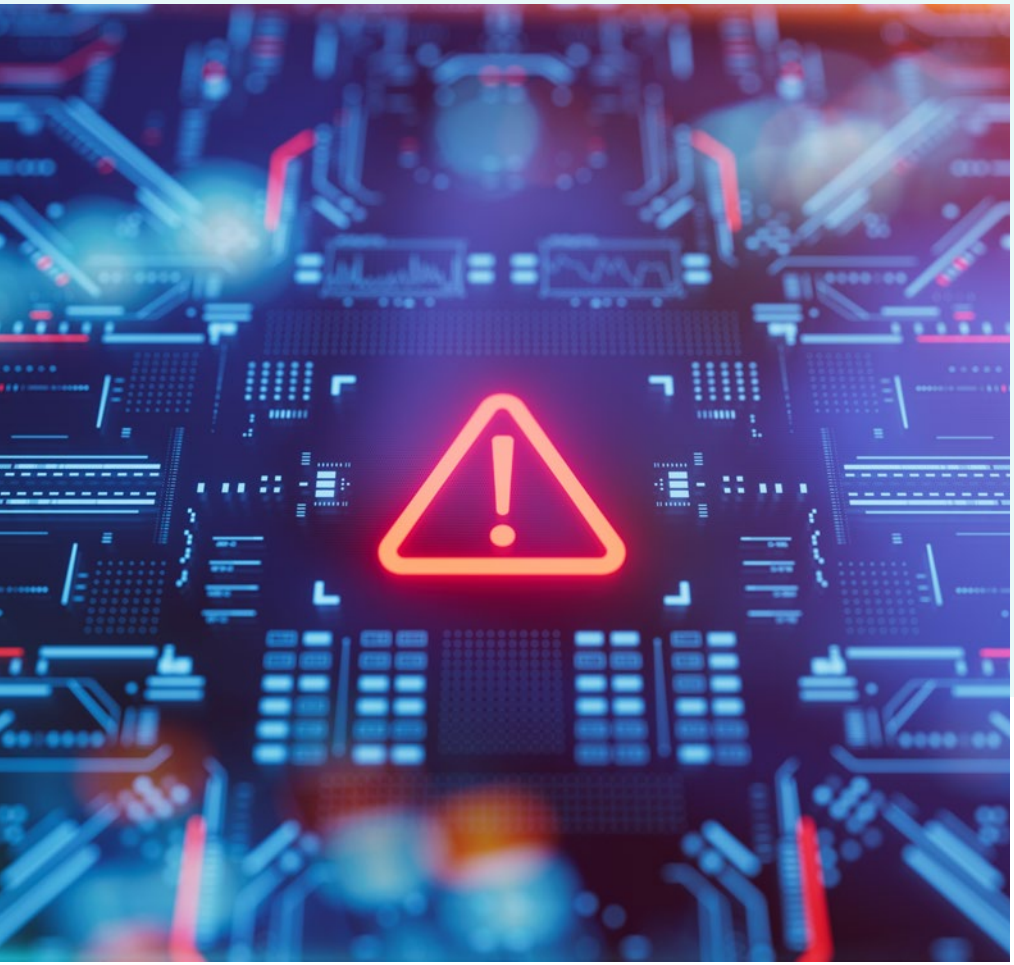
Avoiding blame during a cyberattack within an organisation is crucial because it allows for a more focused and effective response. Cyberattacks are often multifaceted, and assigning blame prematurely can hinder the understanding of the attack's complexity and root causes. Instead, organisations should emphasise shared responsibility for cyber security and foster a culture of learning and continuous improvement.

Blame can have negative psychological, legal and ethical implications, potentially harming morale and collaboration. By focusing on resolving the immediate threat, identifying lessons learned, and preventing future incidents, organisations can enhance their overall cyber security resilience whilst also maintaining a supportive and collaborative environment.

LESSON 6 ›

Don't notify too early

Notifying regulators of a cyber attack too early can be counter-productive, due to inaccuracies, regulatory inquiries, reputational damage, and unnecessary resource diversion. **It is crucial to strike a balance by aligning notification with legal requirements and ensuring a comprehensive understanding of the incident before involving regulators**. This balance has become more challenging, given the short regulatory timeframes for notification (for example, 12 hours in the case of certain critical infrastructure assets under the SOCI Act), as well as the OAIC's heightened expectation that organisations should 'err on the side of notification' (as discussed in section 4.5).



LESSON 7 ›

Expect the unexpected

Cyber threats are diverse, ever-changing, and can exploit unknown vulnerabilities – which means that organisations should anticipate the unexpected. Unpredictable factors such as insider actions, human errors, supply chain risk, regulatory changes and legal consequences, public and media responses, and multifaceted crises, can all play a role in the breach's impact and complexity.

Preparing for the unexpected means having adaptable incident response plans and strategies in place (including 'playbooks' that anticipate different types of incidents); establishing clear roles and responsibilities; and regularly reviewing and testing those plans, strategies and playbooks as the cyber environment changes.

LESSON 8 ›

Place impacted individuals (and not the organisation) at the centre of the investigation

Focus on prioritising impacted individuals over the organisation when preparing breach notifications and deciding on and implementing remediation measures. **This approach gives primacy to privacy rights; assists in compliance with regulatory obligations; and rebuilds trust with customers and the broader community**.

The Red Cross data breach provides an instructive example of this best practice approach.

LESSON 9 ›

Co-operate with regulators

Adopt a proactive and cooperative stance when dealing with regulators. This involves assuming that different regulatory bodies (such as the OAIC, ASIC and the ACCC, and overseas regulators) will communicate and confer with each other. Providing an appropriate degree of transparency is also important, as **giving the right information upfront will avoid the need for regulators to repeatedly seek additional details** – potentially putting them offside.

LESSON 10 ›

Learn from the incident (and from incidents affecting others)

Organisations should extract lessons from data breaches, including those that have affected others. This includes taking a proactive approach to data governance practices (as discussed in section 3) and evaluating the necessity of retaining all data (in compliance with APP 11.2). This proactive approach fosters continuous improvement in data security and responsible data management.

After the Equifax data breach incident of 2017, **Equifax enhanced its cyber security infrastructure, revamped its incident response and compliance procedures, and improved its data governance practices**. This shows how an organisation can use learnings from a significant data breach as an opportunity for growth, resilience and responsible data management.

7. How we can help

We have brought together an unmatched team of cyber security experts under one roof, combining the dynamism of a human-centred, specialised boutique business, with the power of a large Australian law firm.

Find out more 〉

Proactive cyber security

Incident response, digital forensics, breach coaching, and crisis management

Cyber risk Board governance

Privacy and data regulation

Procurement structuring and probity

Software and ICT service procurement

Digital transformations and outsourcing

Telecommunications regulation

IP protection and enforcement

Investigative support

IP commercialisation

Dispute resolution

Strategic risk guidance and integration

8. Meet our team

Report authors

Paul Kallenbach
Partner
Technology and data law
M +61 412 277 134

Susan Kantor
Special Counsel
Technology and data law
M +61 407 545 091

Shannon Sedgwick
Partner
Technology consulting
M +61 481 102 121

Jonathon Blackford
Partner
Technology consulting
M +61 415 837 221

Ashish Das
Partner
Technology consulting
M +61 424 289 204

Christina Graves
Special Counsel
Technology and data law
M +61 421 589 458

Lisa Jarrett
Partner
Technology and data law
M +61 448 880 530

Vanessa Mellis
Partner
Technology and data law
M +61 434 658 811

Nicholas Pascoe
Partner
Technology and data law
M +61 403 857 529

Sonja Read
Partner
Technology and data law
M +61 411 276 772

Tulin Sevgin
Director
Technology consulting
M +61 468 863 620

Amanda Story
Partner
Technology and data law
M +61 423 439 659

In the event of a cyber security incident, please contact MinterEllison's incident response team at

CYBERINCIDENT@MINTERELLISON.COM

Cyber risk and cyber resilience are more pressing than ever for Australian organisations. Heightened geopolitical factors, new regulatory requirements, an increasing prevalence of cyber attacks, and an increasing reliance on technology and data mean that organisations must take proactive steps to build and maintain their cyber resilience.

Paul Kallenbach
Partner, Technology and data law
M +61 412 277 134