PLAN

PROTECT

FORTIFY

Perspectives on Cyber Risk 2022

MinterEllison

Paul Kallenbach
Partner
Technology and Data

> "In the face of heightened geopolitical conflict, intense regulatory focus and a reliance on technology as never before, organisations are facing a unique, perilous and escalating cyber risk landscape."

Foreword
The state of cyber risk in 2022 ›

Welcome to MinterEllison's seventh annual *Perspectives on Cyber Risk* report.

In light of recent global events, a concerted focus on cyber risk and cyber resilience is more pressing than ever for Australian organisations.

With the COVID-19 pandemic now entering its third year, and countries and communities adjusting to the 'new normal' of hybrid work, education and leisure, our reliance on information and communications technology (**ICT**) has continued to increase. This, in turn, has brought with it increased cyber security risks and challenges.

In addition, following Russia's invasion of Ukraine, it was widely reported that Russia employed offensive cyber capabilities early in the war. Reports indicate that Russia has continued in its attempts to disrupt not only Ukrainian networks and systems, but also those of countries that have criticised or sanctioned it.

Even before the onset of hostilities, cyber security had been a keen area focus for the Australian Government, with the passage of significant amendments to Australia's Security of Critical Infrastructure (**SOCI**) legislation in 2021.

However, shortly after Russia's invasion, Australia's Cyber and Infrastructure Security Centre (**CISC**) issued a warning to Australian organisations to urgently adopt an enhanced cyber security posture to address the increased threat of cyber attacks. Remarkably, CISC recommended that Australian organisations should begin *voluntarily* complying with the risk management program obligations in the second tranche of the SOCI legislation, even before that tranche had become law.

Subsequently, in the March 2022 Federal Budget, the Australian Government allocated A$9.9 billion over 10 years to the Australian Signals Directorate (**ASD**) to deliver a Resilience, Effects, Defence, Space, Intelligence, Cyber and Enablers package. This is the largest ever investment in Australia's intelligence and cyber capabilities.

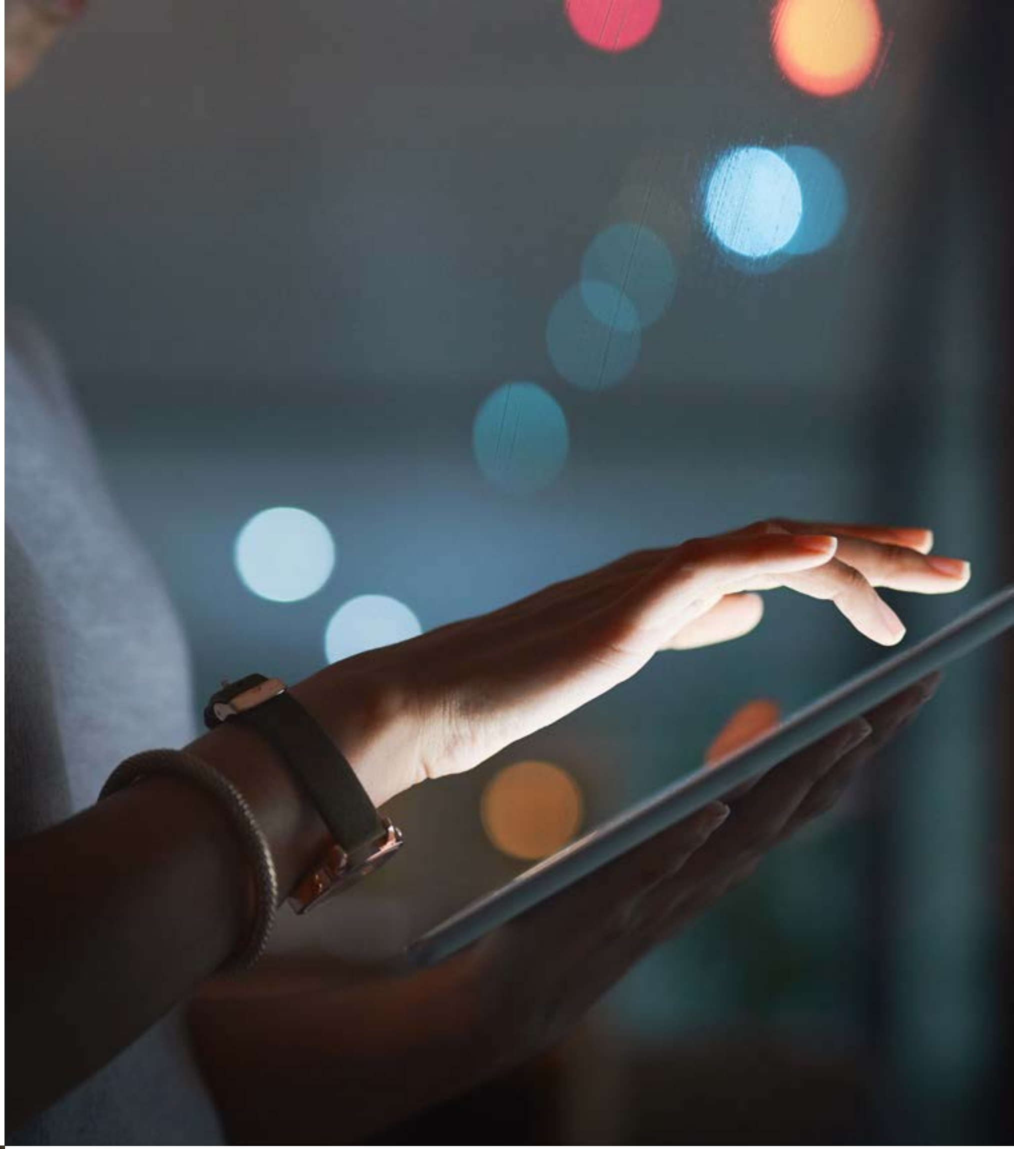
Within this context, there remains much for organisations to address in managing cyber risk – and it's dominating Board and management agendas.

In this year's report, we surveyed executive, legal and IT personnel across almost all sectors of the Australian economy to understand the impact cyber risk is having on their organisations – and what steps they're taking to mitigate the risk.

Survey findings – combined with our interview insights from Chief Information Security Officers, Chief Technology Officers and Chief Digital Officers across a range of sectors – paint a telling picture of escalating cyber risk.

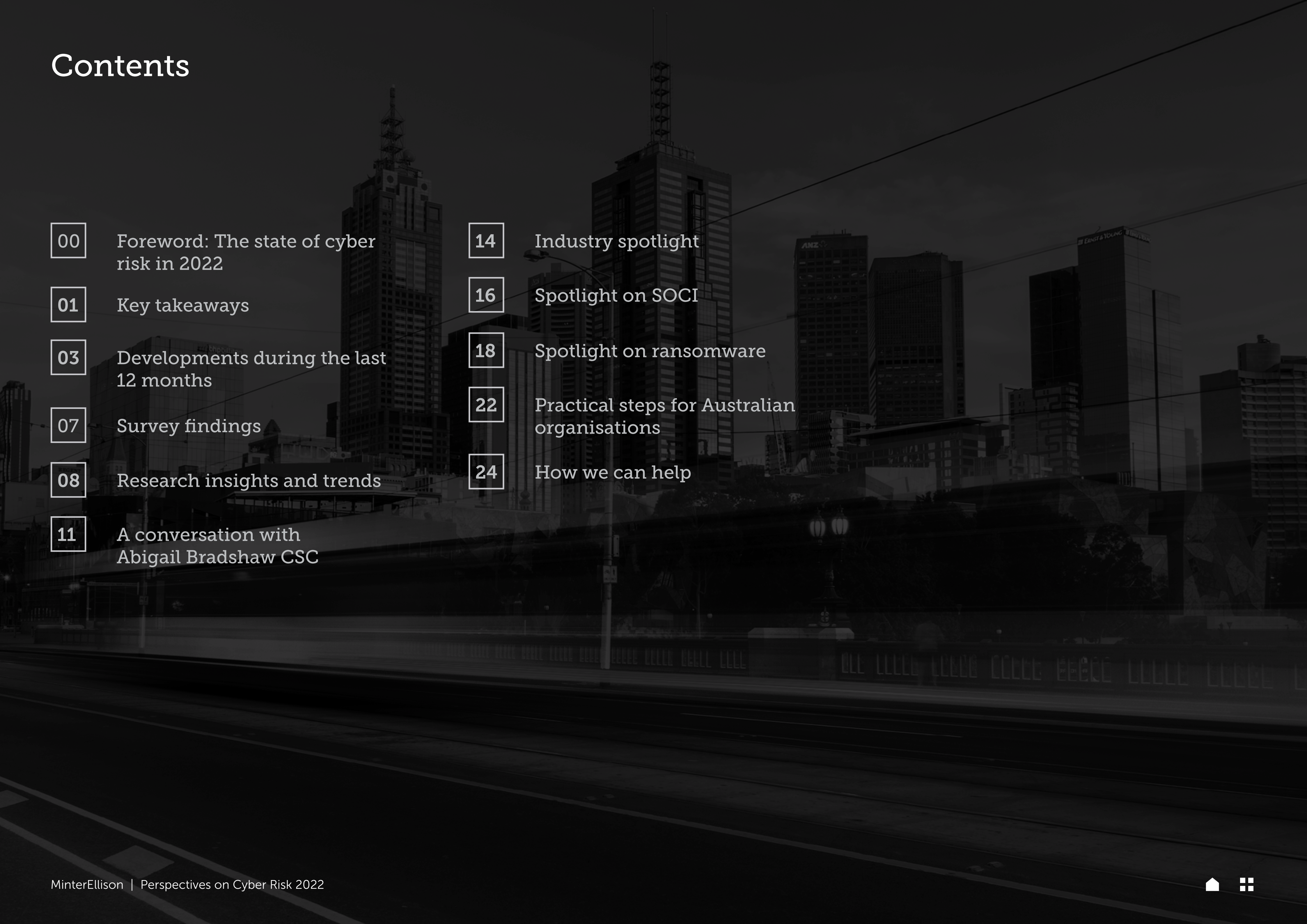
We also share an interview with Abigail Bradshaw CSC, Head of the Australian Cyber Security Centre (**ACSC**), about Australia's cyber security landscape now and in the future.

In addition, we explore recent developments in ransomware, consider the evolving regulatory landscape (including the new SOCI laws), and provide insights from industry leaders on how businesses are managing cyber risk in an increasingly fraught geopolitical context.



"There remains much for organisations to address in managing cyber risk – and it's dominating Board and management agendas."

Contents



Key takeaways

1 With ransomware attacks more prevalent, the cyber risk landscape is ever more threatening

Our survey findings indicate an overwhelming majority (90%) of individuals have personally received an obvious phishing email or ransomware security threat in the last 12 months.

2020-21 saw a 15% increase in ransomware-related cybercrime compared to the previous financial year, as reported in the Australian Cyber Security Centre's Annual Report. In 2020-21, the ACSC responded to nearly 160 cyber security incidents related to ransomware.

Many organisations we interviewed told us they had received additional budget to mitigate a ransomware attack – though few had developed a ransomware playbook to follow should one occur.

Governments around the world are responding. The Australian Government released its *Ransomware Action Plan* in October 2021, which sets out its intention to introduce ransomware-specific laws.

The risks are higher and the impacts increasingly severe – and organisations need to act accordingly.

2 Board awareness and education is a primary concern as the risks escalate and the stakes become higher

56% of respondents told us that cyber security risk ranks high (in the top five) on their organisation's corporate risk register. Increased regulation (including the new SOCI laws) impose onerous new obligations on organisations across many sectors of the economy.

Within that context, Board members are increasingly exposed – both legally and reputationally – if they are not making informed and proactive decisions to manage cyber risk.

While the focus on cyber education may have waned during the peak of the pandemic, the current geopolitical circumstances – together with the ever-increasing volume and sophistication of ransomware and other cyber attacks, and the impact of recent regulatory change – mean there is a renewed and urgent focus on cyber education for Boards and executives, as well as staff at all levels across organisations.

3 Australian organisations are finding it difficult to fill specialist cyber security roles

Many organisations said that finding qualified and experienced IT security personnel continues to be a significant challenge. This is exacerbated by the 'great resignation' and global resourcing issues, but the problem predates those.

Organisations with large volumes of data said they felt particularly exposed by gaps in their resources.

The outcome is evident in organisations' actions. According to our survey, less than 50% of respondents said they have taken steps to assess their cyber security maturity against an established framework.

Despite the resourcing gap, organisations need to urgently adopt appropriate cyber assurance strategies to ensure that they are adequately protected.

4 Cyber insurance is becoming increasingly difficult to obtain – and is not a panacea

Cyber attacks, including those with ransom demands, are increasingly likely, as well as increasingly costly to insurers.

And Abigail Bradshaw, Head of the ACSC, told us that cyber incidents are often under-reported.

In our one-on-one interviews, technology and information security leaders told us that cyber insurance is becoming increasingly more expensive and its coverage more limited – both in terms of the extent of policy exclusions, and the lower available limits.

More generally, leaders recognise that cyber insurance is not (and has never been) a panacea for cyber risk, and that they must continue to take proactive steps to uplift their cyber resilience. They do this by continuing to invest in appropriate detection technologies; by improving their cyber-related policies and processes; by educating and training their Boards, executives and staff on cyber risk; and by mitigating supply chain risk by ensuring that their key suppliers are doing all of these things.

Moreover, if these steps are not taken, it is likely to become more difficult (and expensive) to obtain cyber insurance – or it may even become a risk that cannot be insured against at all.

Developments during the last 12 months

Significant data breaches in Australia and around the world

Data breaches increasingly occur as a result of malicious and criminal attacks. However, human error continues to play a significant part in these attacks, with malicious actors often gaining access to systems by exploiting human mistakes and vulnerabilities.

The number of ransomware attacks has increased significantly – by more than 105% globally over the past 12 months. (See page 18 for a further discussion of the state of ransomware in 2022.)

These latest examples illustrate the scale and cost of the threat that organisations are facing.

- In May 2021, more than 5 billion records held by cyber security analytics firm **Cognyte** were exposed. This included names, email addresses and passwords. Ironically, the information related to user details sourced from previous data breaches, including details from Myspace, Canva, Zoosk and Tumblr data breaches.
- In June 2021, global car manufacturer **Volkswagen** reported a data breach in which customer data – including full names, licence numbers, email addresses, mailing addresses and phone numbers – was exposed online for over 18 months.
- In June 2021, **LinkedIn** announced that the information of over 700 million users had been posted for sale on the dark web, affecting 92% of LinkedIn users, including Australian account holders. Interestingly, much of the information scraped by the unknown actors from LinkedIn was publicly available information.
- In September 2021, US retailer **Neiman Marcus** announced that it had become aware of a data breach that occurred in May 2020, whereby an 'unauthorised party' accessed names, addresses, credit card information and gift card numbers. The intrusion was only detected in September 2021. The breach included the exposure and potential theft of the personal information of 4.6 million customers including over 3.1 million payment cards.
- In November 2021, payroll software provider **Frontier Software** fell victim to a ransomware attack in which the personal information of over 80,000 South Australian public servants was stolen. The attack was orchestrated by Russia-based hacking group Conti, which employs ransomware to encrypt a victim's data before attempting to sell them the decryption key. To date, Conti's haul of ransomware payments is thought to exceed US$32 million.
- In November 2021, **GoDaddy** announced it had been victim to a data breach in which hackers stole information relating to more than 1.2 million of its users. The hackers used a compromised password to access GoDaddy's core systems.
- Australian recruitment company **Finite** was hit by a ransomware attack in December 2021, in which sensitive recruitment details from many Australian businesses were exfiltrated. This included information concerning personal details of job applicants and staff from many large Australian organisations, including Westpac, Coles, Adairs, AMP, NBN Co and various government departments. The attack has been attributed to the Conti group.
- In an unfortunate case of human error, the **ACT Government** was found to have published sensitive health information from nearly 30,000 workers' compensation claims. The data was contained in a spreadsheet that remained publicly accessible on the ACT Government's tender website for more than three years.
- In December 2021, cryptocurrency exchange **BitMart** suffered a large-scale security breach in which cybercriminals withdrew over US$150 million in cryptocurrency assets from the platform. BitMart blamed the attack on a stolen privacy key.

Regulatory developments

Cyber security has been a consistent area of focus for the Australian Government during the last 12 months. We've seen significant legislative change introduced, intended to address increased cyber threats.

Organisations face a number of new hurdles as the cyber security regulatory landscape becomes increasingly complex.

SOCI laws

The *Security Legislation Amendment (Critical Infrastructure)* Act 2021 (**First Amending Act**) came into force in December 2021. The First Amending Act amends the scope of the *Security of Critical Infrastructure Act 2018* (Cth) (**SOCI Act**), which underpins a framework for managing risks relating to critical infrastructure. The First Amending Act extends the obligations under the SOCI Act to a broader range of sectors, now 11 in total compared to the original four:

- communications
- data and storage or processing
- financial services and markets
- water and sewerage
- energy
- healthcare and medical
- higher education and research
- food and grocery
- transport
- space technology
- defence industry.

The First Amending Act also introduces new obligations empowering the Australian Government to issue information gathering and other directions. In addition, if 'switched on' for a particular sector by Ministerial Rules, the new obligations:

- mandate cyber security incident reporting; and
- require certain entities to maintain a register of critical infrastructure assets containing specified information.

The Minister for Home Affairs enacted these Rules on 6 April 2022. The Rules include a three-month transition period for the incident reporting obligations, and a six-month transition period for the asset register obligations.

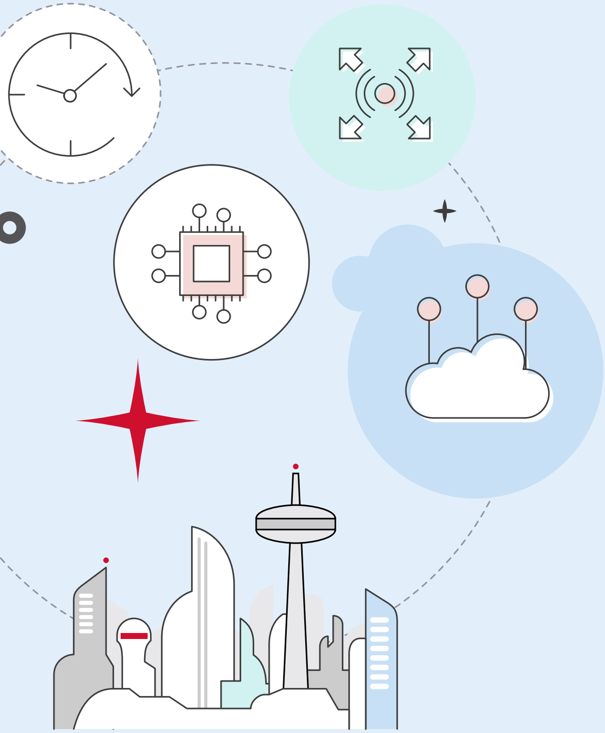
On 31 March 2022, the Australian Government passed the *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022* (**Second Amending Act**). The Second Amending Act introduces the following into the SOCI Act:

- if 'turned on' for particular assets, entities responsible for critical infrastructure assets must adopt and maintain a critical infrastructure Risk Management Program;
- the introduction of a new sub-class of protected assets, called Systems of National Significance (**SoNS**). The Second Amending Act sets out the process by which the Minister can declare a critical infrastructure asset to be a SoNS, and prescribes enhanced cyber security obligations for SoNS; and
- making certain ancillary amendments and insertions to the SOCI Act, such as amending certain definitions relating to critical infrastructure assets specific to each critical sector, and introducing information sharing provisions for regulated entities.

Refer to page 16 for further information about the new SOCI laws.

Ransomware-specific laws

In response to the ever-growing threat of ransomware, the Minister for Home Affairs released the Ransomware Action Plan, followed by a Bill that would implement key aspects of the Plan. Refer to page 20 for a discussion of the Plan and other ransomware-related developments in 2022.



ASIC Market Integrity Rules

In March 2022, the Australian Securities and Investments Commission (**ASIC**) introduced the *ASIC Market Integrity Rules (Securities Markets and Futures Markets) Amendment Instrument 2022/74*. These new Rules will commence on 10 March 2023, and will:

- impose additional obligations on market participants and operators in relation to technology and operational resilience; and
- reinforce ASIC's broader regulatory focus on deterring inadequate systems and uplifting operational governance and controls.

Some of the organisations that will be subject to the new Rules are already required to comply with Australian Prudential Regulation Authority (**APRA**) *Prudential Standard CPS 234 Information Security*. However, the Rules will nevertheless impose a further layer of information security and operational resilience obligations on these and other organisations.

Draft Privacy Act amendments

The exposure draft of the *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill* 2021 (**Online Privacy Bill**) was released in October 2021. The Bill proposes to introduce a new binding online privacy code for social media and certain other online platforms. It would also increase the penalties and enforcement powers applicable under the *Privacy Act 1988* (Cth) (**Privacy Act**). For example, the draft legislation proposes to increase the maximum civil penalty for a serious and/or repeated interference with privacy to 2,400 penalty units for an individual (which currently equates to A$532,800), or for a body corporate an amount not exceeding the greater of:

- A$10 million; or
- three times the value of a benefit obtained by the body corporate from the conduct that was a serious or repeated interference with privacy; or
- 10% of domestic annual turnover, if a value attributable to the interference cannot be determined.

Other proposed enforcement mechanisms include new powers conferred on the Office of the Australian Information Commissioner (**OAIC**) to issue enforcement notices.

Concurrently, the Commonwealth Attorney-General released the next round of consultation on the broader Privacy Act review, through its Discussion Paper. This Paper (which follows an earlier Issues Paper) sought submissions on the broader proposed amendments to the Privacy Act, as recommended by the Australian Competition and Consumer Commission in its *Digital Platforms Inquiry Final Report*. The Discussion Paper, among other things, sought feedback on the effectiveness of the Notifiable Data Breach Scheme under Part IIIC of the Privacy Act.

The consultation periods for the Online Privacy Bill and Discussion Paper have now closed, and we await the Australian Government's response.

Trends in regulatory enforcement

The OAIC continues to pursue Facebook in Federal Court proceedings and has issued a robust warning to organisations that seek to rely on biometrics to exploit personal information.

Facebook, Inc.

In February this year, the Full Bench of the Federal Court rejected Facebook, Inc.'s appeal to set aside an earlier ruling granting the OAIC leave to serve legal documents on the US-based entity.

The earlier ruling found that the OAIC had established a *prima facie* case that Facebook, Inc. was carrying on business in Australia, on the basis that it was collecting and holding personal information in Australia at the relevant time, and was therefore subject to the requirements of the Privacy Act.

The OAIC initially filed proceedings against Facebook in March 2020, alleging that the platform committed serious and/or repeated interferences with privacy in connection with the Cambridge Analytica scandal.

Facebook has since filed an application for special leave to the High Court, so this initial question is not yet fully litigated.

The case is particularly significant because it is the first penalty proceeding under the Privacy Act that will consider whether an organisation's actions, in this case Facebook's, amounted to a serious and/or repeated interference with Australians' privacy.

Biometrics

As biometric technology continues to develop and its use becomes more widespread, we have seen the OAIC pay particular attention to the adoption of this technology and its impact on Australians' privacy.

In the past 12 months, the OAIC has issued determinations regarding the collection of sensitive biometric information by organisations.

Most notably, in November 2021, the OAIC issued a determination that Clearview AI had breached the Privacy Act by scraping biometric information from the internet and disclosing it through its facial recognition tool.

Clearview AI's facial recognition tool scrapes social media platforms and other publicly available websites to obtain facial images. The tool allows the user to upload an image that is then cross-referenced against its database to assist with identification of the individual.

In her determination, Australian Information Commissioner Angelene Falk warned that "by its nature, this biometric identity information cannot be reissued or cancelled and may also be replicated and used for identity theft. Individuals featured in the database may also be at risk of misidentification."

The OAIC has therefore put organisations on notice that they should carefully consider whether the use of biometrics is necessary for their functions and activities, and should ensure that any such use meets the expectations of Australians for the protection of their personal information.

Additionally, the OAIC issued a determination that the Australian Federal Police (**AFP**) failed to comply with its privacy obligations in its use of the Clearview AI platform. Among other things, Commissioner Falk found that the AFP did not have appropriate systems in place to identify and track the use of technology involving personal information handling, and failed to complete a privacy impact assessment before using the platform. The AFP has been directed to engage an independent third-party assessor to review any residual deficiencies in its practices in relation to privacy assessments.

Survey findings

In February 2022, we conducted our annual Cyber Risk survey. We received responses from executive, legal and IT personnel across almost all sectors of the Australian economy. Key insights from the results were:

90% of respondents

have personally received an obvious phishing email or ransomware security threat in the last 12 months

<50% of respondents

said they have taken steps to assess their cyber security maturity against an established framework

56% of respondents

said that cyber security risk ranks as high risk (top five) on their organisation's corporate risk register

25% of respondent organisations

were subject to at least one cyber security incident in the past 12 months that compromised their systems or data

More respondent organisations said they are regularly testing their cyber security plans (55% in 2021 compared with 59% in 2022)

Of those who have taken steps to assess their cyber security maturity against an established framework, the ASD's Essential Eight Maturity Model was the most common framework adopted

Methodology

Data is compiled from our annual online survey conducted in February 2022. The survey was first conducted in 2016. In 2022, half of the respondents were legal counsel, while others were board members, CIOs, directors and other specialists. In addition, data incorporates polling results obtained during MinterEllison's cyber law update webinar, held as part of the CPD Legal Studio in February 2022, and results from the 2022 MinterEllison Financial Services in Focus survey.

The survey results indicate that malicious cyber activity is prevalent, with a quarter of respondent organisations being subject to a cyber security incident that compromised their systems or data, and 90% of respondents having personally received an obvious phishing email or ransomware security threat in the past 12 months. This suggests that there is a significant volume of attempted cyber attacks, but also that individuals are becoming more adept at recognising suspicious cyber activity. While many organisations consider cyber security risk to be a high risk for their organisation, there are additional measures that organisations can and should take in order to address the risk. Notably, less than half of respondents said they have taken steps to assess their cyber security against an established framework. We spoke with technology and information security leaders for their insights on cyber security issues (see page 9). A common recommendation among these leaders was for organisations to benchmark their cyber security practices against external established framework, such as the ASD's Essential Eight Maturity Model.

We also saw some improvements from last year's survey results, with an increase in the percentage of respondent organisations who say they are regularly testing their cyber security plans. Conversely, 41% of respondent organisations either do not regularly test their cyber security plans or are not sure whether they do so. We strongly encourage all organisations to continue to prioritise cyber security and implement a regular testing program of their plans to mitigate evolving cyber security risk.

Research insights and trends

Areas of focus

In addition to our quantitative survey, we spoke with technology and information security leaders across a range of industries to gain a more in-depth, qualitative understanding of the current cyber issues of focus and the measures that they are implementing. Together, this research identified seven key trends:

1 Increased focus on ransomware threats

The ever-increasing risk of a ransomware attack is a key focus for IT security personnel, and organisations are implementing a range of technical, personnel and policy measures to mitigate the risk of ransomware attacks and prepare for an attack should it occur. Although 90% of our surveyed respondents reported receiving an obvious phishing email in the last 12 months, only one of the industry leaders we spoke with told us that their organisation had suffered a ransomware attack in previous 12 months.

However, all of the organisations we spoke with recognised that ransomware threats pose a significant risk to their organisation. Some organisations said that they have received additional budget to support their efforts in mitigating this threat.

Various organisations have engaged specialised third parties to manage endpoint security, and have implemented enhanced technical controls (such as data and network segmentation) in anticipation of a ransomware attack.

Interestingly, almost all organisations told us that they had not yet developed a specific ransomware policy or playbook to address (for example) escalations and decision-making authorities; the legal and reputational factors to be considered when making a ransomware payment; and employee, customer and regulator communications strategies should a ransomware attack occur.

2 Focus on mitigating risks posed by the supply chain

A number of industry leaders focused on the supply chain as a key risk for their organisation.

They said that they are addressing this risk by implementing additional technical and organisational controls (including by more carefully vetting their suppliers and including additional rights in their contracts); and by exercising current contractual audit rights, for example, by issuing IT security-based questionnaires to their key suppliers.

3 Concern regarding geopolitical threats

Some organisations expressed specific concerns about the heightened threat of cyber attacks in light of the attack on Ukraine, and are implementing additional technical measures to protect their systems in light of this.

4 Resourcing constraints are a concern

Many organisations told us that finding qualified and experienced IT security personnel continues to be a significant challenge, exacerbated also by the 'great resignation'. Organisations with large volumes of data (including sensitive data) said they felt particularly exposed by gaps in their resources.

5 Board education is a renewed focus

For some organisations, their focus on cyber education for Board members and the conduct of desktop exercises waned during the last two years as a consequence of their focus on pandemic-related issues. However, given the current geopolitical circumstances, the heightened risk of cyber attacks and a more onerous regulatory landscape, leaders told us they now have renewed focus on cyber education across the organisation.

56% of survey respondents

said that cyber security risk ranks as high risk (top five) on their organisation's corporate risk register

All of the leaders interviewed now run multifaceted cyber security education programs for executives and other employees, including regular phishing simulations. They also said they conduct regular testing of cyber incident response plans, as well as regular reporting to the Board on cyber security and cyber resilience. Our survey identified that 59% of respondent organisations are regularly testing their cyber security plans, up from 55% in 2021.

6 Leveraging of external frameworks and networks

Industry leaders told us that they are either formally or informally benchmarking their cyber security practices against the ASD's Essential Eight Maturity Model or the US National Institute of Standards and Technology (**NIST**) Cybersecurity Framework.

<50% of survey respondents

said they have taken steps to assess their cyber security maturity against an established framework. Of those who have, the Essential Eight was the most common framework adopted.

Almost all of our interviewees have joined industry IT security groups and the ACSC's partner network to keep up to date with current cyber threats and trends.

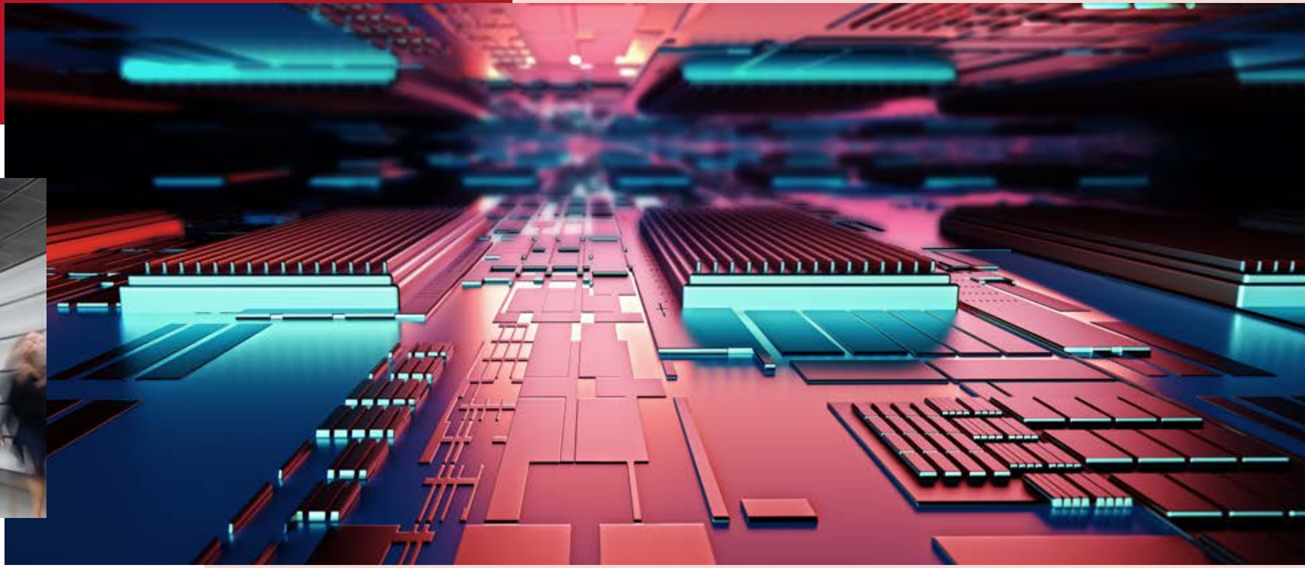
7 Changes in cyber and other insurance policies

Organisations told us of the challenges they had faced in obtaining or renewing cyber insurance. In one case, a long-standing insurer had declined to renew the organisation's cyber policy, causing the organisation to scramble to find a replacement policy in order for it to meet downstream contractual requirements.

Some leaders told us that their insurers had increased their premiums, narrowed the scope of coverage through new policy exclusions and decreased their cyber insurance limits. Some also told us that their insurers are reviewing their business interruption and other policies, and are imposing specific exclusions relating to cyber in those policies.

Lessons from industry leaders in managing cyber risk

1. Develop **ransomware-specific safeguards** and policies
2. Conduct **regular tests of cyber incident response plans** and update those plans as necessary
3. Conduct **regular and tailored cyber attack simulation exercises**
4. Conduct tailored **cyber security education programs** for the Board and executives, as well as for employees across the organisation
5. Focus on **mitigating supply chain risk**, including by implementing appropriate technical and organisation controls
6. **Benchmark the organisation's cyber security practices** against external standards and frameworks – including by reviewing the organisation's approach to the identification of critical assets; patching; application whitelisting; adoption of multifactor authentication; implementation of network and data segmentation; and reviewing and improving backup strategies
7. **Join industry groups and networks** to keep up to date with current cyber threats and trends



A conversation with Abigail Bradshaw CSC

Head of the Australian Cyber Security Centre

In early 2022, we asked the Head of the ACSC about Australia's cyber risk landscape – the trends, the challenges and the ACSC's advice. This is what she had to say.

Q Describe the ACSC's role in assisting organisations who have suffered a cyber attack, and the advantages of notifying the ACSC of an attack.

The ACSC, which sits within the ASD, leads the Australian Government's efforts to improve cyber security. Our role is to help make Australia the most secure place to connect online. We provide technical advice and assistance, including remediation advice, and raise advisories and alerts to warn other organisations, business sectors or the entire nation if necessary. Reporting cyber incidents is vital to develop a national threat picture, alert other potential victims and provide Australians with the best cyber security advice.

Research indicates that cyber incidents are often under-reported. Not reporting cyber incidents can hamper an organisation's efforts to respond or recover from a cyber incident. It also diminishes the value of any threat intelligence that the ACSC might use to help other Australian businesses and individuals. When cyber incidents are reported, the ACSC can support victims and leverage the unique experience built over 75 years by the ASD, including a capacity to strike back. The ACSC can also refer incidents to law enforcement or other investigating agencies where appropriate.

Q Has the ACSC identified any trends in cyber attacks over the last 12 months? If so, please describe them.

Our Annual Cyber Threat Report 2020-21 identified a number of trends in the threat environment. There was a 15% increase in ransomware-related cybercrime reported via the ACSC's ReportCyber tool in FY 2020-21, compared to the previous financial year. The ACSC also responded to nearly 160 cyber security incidents related to ransomware.

Our data shows one-quarter of ACSC-recorded cyber incidents in FY 2020-21 affected Australia's critical infrastructure, including essential services such as education, health, communications, electricity, water and transport. In 2021, a ransomware attack affected one of Melbourne's larger metropolitan public health services. An effective and coordinated incident response minimised disruption.

In December last year, the ACSC alerted Australians to the significant Apache Log4j vulnerability. We saw malicious actors hunting for vulnerabilities to exploit. We wasted no time in providing advice on our website. If unaddressed, the vulnerability could allow cybercriminals to break into an organisation's systems, steal login credentials, extract sensitive data and infect networks with malicious software.

Australia also remains a regular target of state-sponsored actors who rapidly exploit vulnerabilities, including weaknesses in software supply chains. State-sponsored threat actors employ a wide range of tactics to target Australian networks, seeking sensitive information that could be used to weaken Australia's competitive advantage and degrade national security.

A conversation with Abigail Bradshaw CSC
Head of the Australian Cyber Security Centre

Q What does the ACSC perceive to have been the biggest challenges for organisations in responding to cyber attacks over the past 12 months?

Cyber threats and cybercrime against Australia continue to evolve. These threats include an increase in sophisticated ransomware attacks, data breaches, online fraud and business email compromise (**BEC**). In September 2020, an Australian hedge fund was subject to BEC. This involved false invoices with the company transferring A$8.7 million to bank accounts controlled by the offenders. The business was forced to go into receivership and the attack resulted in bankruptcy. This was likely Australia's first bankruptcy case as a direct result of cybercrime.

We're also seeing the effects of the COVID-19 pandemic, including in the way organisations have shifted many processes and services online, and moved to remote work arrangements. Some remote working solutions were hastily implemented, leaving organisations vulnerable to cyber threats because employees were using old or unpatched devices, and not using virtual private networks (**VPNs**). The ACSC, through its Partnership Program and Joint Cyber Security Centres, can assist Australian organisations navigating cyber security challenges.

Q From the ACSC's interactions with organisations following a cyber attack over the last 12 months, how does the ACSC perceive organisations' preparedness to respond to cyber attacks? Has this changed over the last few years?

In FY 2020-21, many of the compromises experienced by Australian organisations could have been mitigated by taking simple steps to protect systems. The ACSC, in partnership with cyber security agencies in the UK and the US, issued a joint advisory after observing an increase in sophisticated, high-impact ransomware incidents. Cybercriminals were gaining access to networks via phishing, by using stolen Remote Desktop Protocol credentials or brute force, and by exploiting software vulnerabilities.

In light of the increasing prevalence of cyber attacks, it is critical that entities have measures in place to respond to cyber security incidents, to protect not only their organisations, but also their clients and customers. Organisations need to be asking questions of themselves and those they deal with, including for example how they will respond to an incident, whether they have a regular patching program and whether they have a practised cyber incident response plan in place. Large organisations also need to contemplate vulnerabilities that arise within their supply chains.

There has been a big surge in the number of Australians joining the ACSC Partnership Program, which has over 2,100 Network Partners, over 3,300 Business Partners and over 78,000 Home Partners. Partners can share threat intelligence and tips, and participate in workshops and cyber exercises with Australia's fast-growing cyber security community.

In August 2021, the ACSC hosted Aqua Ex, a major cyber exercise involving over 60 entities from Australia's critical infrastructure community. ACSC's pilot Critical Infrastructure Uplift Program (**CI-UP**) is also helping critical infrastructure organisations to evaluate their cyber security maturity, and prioritise and implement risk mitigations.

The strong engagement we have had from the community and industry suggests there is an increasing awareness of the need to taker cyber seriously, and when we work together we can make positive changes to Australia's cyber ecosystem.

> "
>
> Preparing to respond to a cyber attack starts with **leadership** and the **right culture**."

Q What is the ACSC's advice to guard against ransomware attacks?

Ransomware is one of the most significant cyber threats currently facing Australians and Australian organisations. It is a global threat. When it comes to defending against ransomware, it is imperative that organisations raise the defences early or face the consequences. We have published the Ransomware Attack Prevention and Protection Guide on cyber.gov.au, to teach all Australians how to mitigate ransomware threats.

Investing in preventative cyber security measures is more cost-effective than the comparative costs incurred when attempting to recover from a ransomware incident. Update devices and turn on automatic updates, use multifactor authentication, maintain current backups (preferably stored offline), protect systems with strong passphrases and access controls, and have an incident response plan. We do not recommend paying ransom demands, as it does not guarantee a victim's files will be restored. Nor does it prevent the publication of any stolen data, or stop it being sold for use in other crimes.

To protect Australians and combat this global threat, the Australian Government launched the Ransomware Action Plan, which builds on Australia's Cyber Security Strategy 2020.

Q What is your advice to organisations on how best to prepare for responding to cyber attacks?

Preparing to respond to a cyber attack starts with leadership and the right culture. Effectively preparing for a cyber incident requires the full involvement of the organisation, from the board to the public relations team and frontline workers. The best prepared organisations have robust disaster recovery plans that consider three key elements:

1. Operational contingencies, should some or all of your systems go offline. How will you manage operations like logistics or public communication?
2. Exercising incident response plans with the whole executive and key functions of your organisation.
3. Testing backups regularly. Much like organisations run fire drills, backups should be tested and include a full restoration.

Implementing the ASD's Essential Eight Maturity Model is the best approach to in-depth defence. Based on the ACSC's experience in producing cyber threat intelligence, conducting penetration testing and assisting organisations, the Essential Eight is proven to help organisations minimise cyber risk.

Cyber.gov.au is a one-stop shop for guides and advice, and is the gateway to the ACSC's Partnership Program. The ACSC urges all Australian individuals and organisations to report cybercrime and cyber incidents to ReportCyber, contactable 24/7 via email asd.assist@defence.gov.au or by calling the Australian Cyber Security Hotline on 1300 CYBER1 (1300 292 371).

Industry spotlight

Energy and Resources

SOCI laws

The energy and resources industry is a critical infrastructure sector. The Australian Government has 'switched on' the incident reporting and asset register obligations, and proposes to 'switch on' risk management obligations for this sector.

Australian Energy Sector Cyber Security Framework (AESCSF) extended to liquid fuels sector

The AESCSF is a program developed by the Department of Industry, Science, Energy and Resources in partnership with the Australian Energy Market Operator to assess cyber security maturity in the energy sector and to complement SOCI law reform. The AESCSF originally covered electricity and gas markets, but will be extended to include the liquid fuels sector.

Financial Services

CPS 234 Tripartite Reviews

Regulated entities may be required to engage third-party auditors to undertake a CPS 234 compliance audit, with the results to be reported to the organisation's Board and to APRA.

Changes in cyber insurance

Given the significant rise in cyber attacks and insurance payouts, cyber insurers are reviewing policies to increase premiums, and are also narrowing coverage (by expanding policy exclusions and lowering available limits).

SOCI laws

The financial services and markets industry is a critical infrastructure sector. The Australian Government has 'switched on' the incident reporting obligations for this sector, as well as the asset register obligations for some impacted assets. The Australian Government also proposes to 'switch on' the the risk management program obligations for some impacted assets in this sector.

ASIC Market Integrity Rules

These new Rules will commence on 10 March 2023, and will:

- impose additional obligations on market participants and operators in relation to technology and operational resilience; and
- reinforce ASIC's broader regulatory focus on deterring inadequate systems and uplifting operational governance and controls.

Government

Key target for state-sponsored attacks

Government infrastructure is at particular risk of state-sponsored cyber attacks in light of the current situation in Ukraine.

Higher education

SOCI laws

The higher education industry is a critical infrastructure sector. The Australian Government has 'switched on' the incident reporting obligations for this sector.

Continued threat of foreign interference

The report on the parliamentary inquiry into national security risks affecting the Australian higher education and research sector was published in March 2022. The Australian Security Intelligence Organisation considers the sector a key target for foreign interference. The report recommends further security measures be implemented – including training, additional processes and government assistance – to address this threat.

Infrastructure

SOCI laws

Transport is the largest component of the infrastructure sector. The Australian Government has 'switched on' the incident reporting and asset register obligations for transport assets. Related laws were introduced to Parliament under the *Transport Security Amendment (Critical Infrastructure) Bill* 2022, which lapsed when Parliament was prorogued ahead of the election.

Delivery phase and the transition into operation

Many organisations in this sector rely on operational technology to monitor and control physical processes or devices. These devices create significant efficiencies for the sector but also expose the sector to a growing risk of cyber attacks affecting critical infrastructure assets. With Building Information Modelling likely to be used on every major project there are increasing volumes of very useful and detailed information shared. This flow varies over the lifecycle of a build and into subsequent operation and it is critical that this data is managed accordingly.

End users need to have confidence in the management of personal data

Great infrastructure provides end users with a seamless and efficient experience. Many assets are increasingly reliant of the gathering and application of personal data sets to influence operational efficiency. End users have to be comfortable with the trade-off i.e. that data is collected for the purpose at hand without being exploited for other commercial or non-commercial uses.

Health

Key target for malicious attacks

Health service providers are a key target for malicious attacks. From January to June 2021, the OAIC received the most data breach notifications from this sector, of any sector, arising from malicious attacks.

SOCI laws

The healthcare industry is a critical infrastructure sector. The Australian Government has 'switched on' the incident reporting and asset register obligations, and proposes to 'switch on' the risk management program obligations for impacted assets in this sector.

Insurance

The Insurance Council of Australia (ICA) released its Cyber Insurance: Protecting our way of life, in a digital world discussion paper on 28 March 2022, which sets out the insurance implications of cyber incidents on Australian businesses and recommendations for a sustainable cyber insurance market.

According to the ICA, cyber insurance awareness is low within the Australian business economy, and the combination of a small premium pool and increasing sophistication and maliciousness of some cyber attacks has put significant pressure on insurers as well as businesses.

The ICA recommends that policyholders work closely with insurers to ensure they understand the extent of cyber coverage, and has recommended (among other things) that the Australian Government develop a single cyber security framework to help drive best practice in cyber security across the Australian economy.

Spotlight on SOCI

Overview of SOCI laws

Government assistance measures

Following an incident, government is empowered to issue information gathering and provision of support directions

To be used as a measure of last resort

Applies to all sectors

Register of critical infrastructure assets

Reporting entities must report details about entity and asset to CISC

Reporting required at time of registration and must be kept updated

Mandatory cyber incident reporting

Incident with significant impact on availability of assets – report to ACSC with 12 hours

Incident with relevant impact on availability of assets – report to ACSC with 72 hours

Laws passed

These requirements have been 'turned on' for some assets through Ministerial Rules that took effect on 8 April 2022 with:
3 month transition for incident reporting obligations
6 month transition for asset register obligations

Risk management programs

Responsible entities required to adopt and maintain a Risk Management Program

Annual compliance certification to CISC

Enhanced security measures

Asset is declared a System of National Significance and notified. Could be:

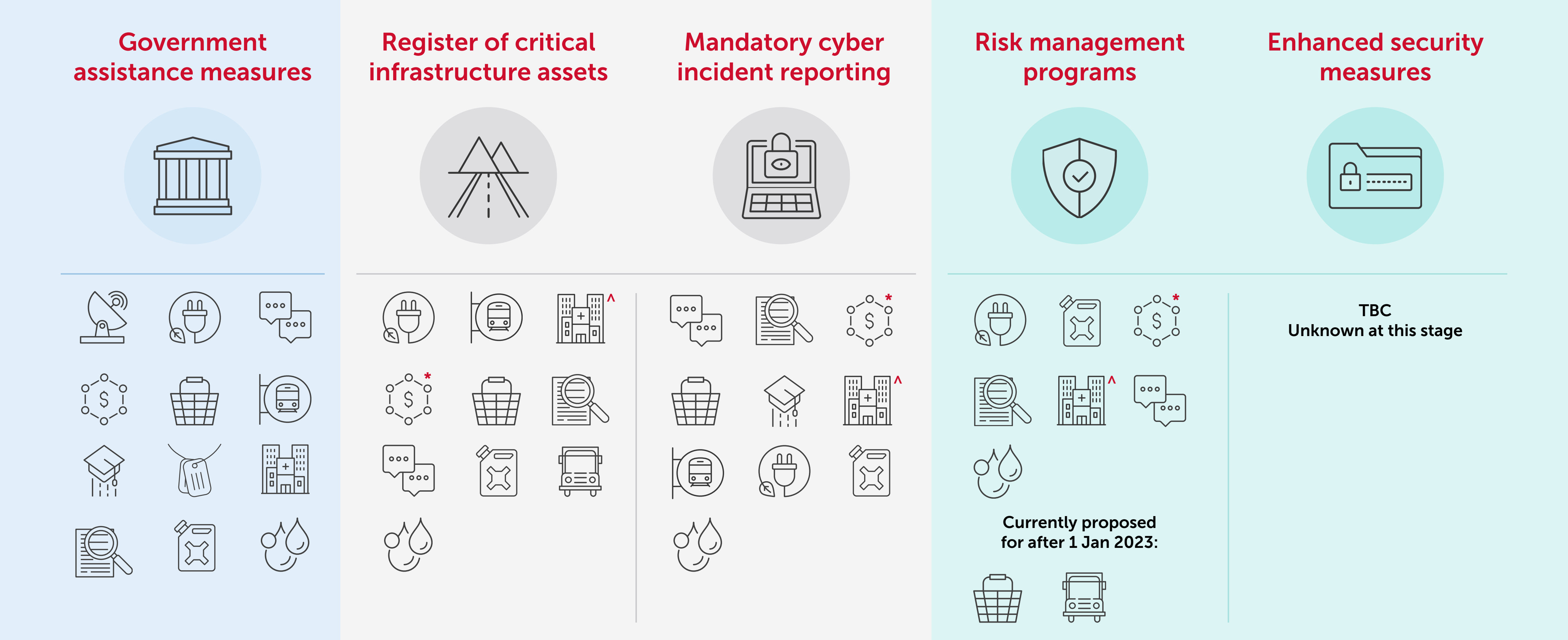
- Prepare incident response plan
- Undertake cyber security exercises
- Undertake vulnerability assessments
- Provide systems information

Laws passed, awaiting rules

Risk Management Program law passed.
Awaiting Ministerial Rules to 'turn on' the Risk Management Program obligations for some assets, but government has recommended implementing now.

Spotlight on SOCI

Overview of SOCI laws



Government assistance measures

Register of critical infrastructure assets

Mandatory cyber incident reporting

Risk management programs

Currently proposed for after 1 Jan 2023:

Enhanced security measures

TBC
Unknown at this stage

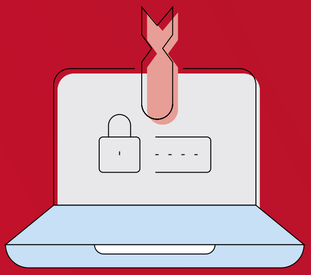
Legend:

* Payment systems only | ^ Critical hospitals only

Space Technology	Energy (Electricity and Gas)	Communications	Transport	Healthcare and Medical	Water and Sewerage	Financial Services and Markets	Food and Grocery	Higher Education and Research	Defence	Data storage or Processing	Freight infrastructure and services	Liquid fuel

Spotlight on ransomware

At a glance



Nearly

20 per second

Number of attempted ransomware attacks globally in 2021

(Source: SonicWall 2022 Cyber Threat Report)

15%

The percentage increase in ransomware reports by Australian organisations in FY 20-21 compared with the previous financial year

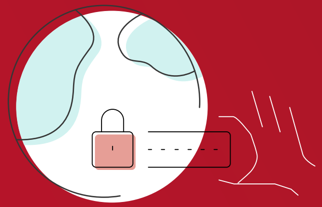
(Source: Australian Cyber Security Centre)

623.3m

The number of ransomware attacks globally in 2021

(Source: SonicWall 2022 Cyber Threat Report)

105%



The percentage increase in ransomware attacks globally in 2021 compared with 2020

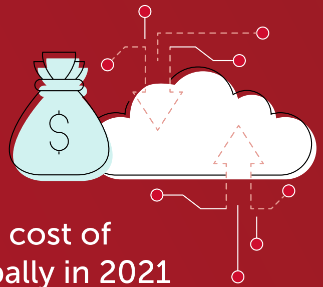
(Source: SonicWall 2022 Cyber Threat Report)

US $6m

Estimated average ransomware demand levied against US companies in 2021

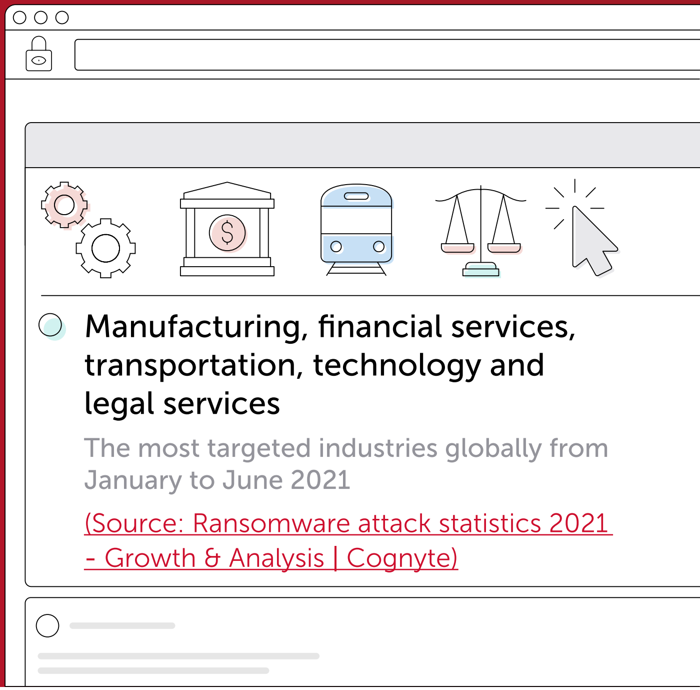
(Source: Mimecast)

US $20b



The estimated combined cost of ransomware attacks globally in 2021

(Source: Cybersecurity Ventures)



Manufacturing, financial services, transportation, technology and legal services

The most targeted industries globally from January to June 2021

(Source: Ransomware attack statistics 2021 - Growth & Analysis | Cognyte)

Trends in ransomware

Continued risk of attacks on Australian organisations

Consistent with global trends, the ACSC has continued to observe cybercriminals successfully using ransomware to disrupt business operations and cause reputational harm to Australian organisations. Increasingly, however, attackers are not only demanding payment to enable the organisation to regain access to its data, but also carrying out secondary extortions by threatening to release on the dark web.

Ransomware-as-a-Service (RaaS) is expected to increase

RaaS involves operators leasing out or offering subscriptions to their malware creations to others (known as 'affiliates') for a fee – such as a monthly subscription fee or a percentage of successful extortion payments. The increasing prevalence of ransomware attacks may be attributed to, at least in part, the increased accessibility afforded by this model. RaaS operators such as DarkSide (responsible for an attack on the Colonial Pipeline in Texas in May 2021) and REvil (behind the attack on JBS Foods in May 2021 – see below) offer RaaS to affiliates through the dark web and Twitter.

The US Federal Bureau of Investigation (**FBI**) issued its first alert about a ransomware 'affiliate' in August 2021. In February 2022, the FBI released a further alert, warning organisations that BlackByte, a Raas provider, has begun targeting critical infrastructure sectors.

The use of open-source software (OSS) presents an ongoing risk for exploitation by ransomware criminals

OSS is commonly leveraged by both in-house and external developers across the globe. As a consequence of its widespread use, OSS presents a particular risk of exploitation by ransomware criminals.

In December 2021, malicious code (referred to as Log4Shell) was discovered in Log4j – an ubiquitous OSS JavaScript library used by numerous cloud-based services – which allowed hackers to remotely access and take control of affected systems.

On 8 March 2022, the maintainer of node-ipc, an OSS JavaScript library that is downloaded approximately a million times a week, released an update containing 'protestware'. The effect of the update was that if the IP address of the user was geocoded as Russian or Belarussian, the software overwrote any data encountered in the user's filesystem with heart symbols. The action was intended as a protest against Russia's invasion of Ukraine.

While these incidents did not result in ransomware attacks, they demonstrate the vulnerabilities of OSS and the risk of exploitation by malicious actors, which could result in attempted ransomware attacks in the future.

Ransomware will continue to impact cyber insurance

Organisations' ever-increasing reliance on ICT and the associated rise in ransomware attacks is continuing to shape the cyber insurance landscape. In the past, cyber insurance was often purchased as an add-on to other standard commercial insurances. However, as ransomware attacks have increased, so have cyber reinsurance rates, by up to 40% in FY 2020-21.

Notably, while many cyber insurance policies offered in Australia continue to provide coverage for the payment of ransoms, insurers are reassessing this position. In addition, insurers are limiting coverage in a portfolio if a business isn't able to demonstrate having appropriate cyber security measures in place. Ultimately, cyber insurance is just one tool within a broader arsenal that organisations should employ to mitigate against the impact of ransomware attacks.

Ransomware regulatory developments

Local developments

The Australian Government has acknowledged the growing threat that ransomware poses to Australian businesses, individuals and infrastructure. In October 2021, the Minister for Home Affairs released the Government's Ransomware Action Plan. The Plan sets out the Government's intention to introduce ransomware-specific legislative reforms, including:

- the imposition of specific mandatory ransomware incident reporting;
- the introduction of a standalone offence for all forms of cyber extortion; and
- the introduction of a standalone offence for cybercriminals seeking to target critical infrastructure assets (as defined in SOCI law).

The Plan came after the Federal Opposition introduced the Ransomware Payments Bill 2021 to Parliament in August 2021, which proposed to make it mandatory for large business and government entities to notify the ACSC if they made a ransomware payment.

While the Bill has since been withdrawn, on 17 February 2022, the Australian Government introduced the *Crimes Legislation Amendment (Ransomware Action Plan) Bill* 2022 into Parliament. The Bill aims to implement some of the key aspects of the Ransomware Action Plan. In addition to the reforms outlined above, the Bill introduces a standalone offence of dealing with data obtained by unauthorised access or modification, and an aggravated offence for buyers and sellers of ransomware to deter the development of RaaS markets.

Notably, the Bill does not introduce mandatory ransomware incident reporting requirements or any new offences expressly criminalising the payment of a ransom. The Bill lapsed when Parliament was prorogued.

International developments

Australia recommitted to the Five Eyes group in April 2021. Five Eyes consists of representatives from Australia, New Zealand, Canada, the United States and the United Kingdom. Acknowledging the global nature of the challenge, Five Eyes works collaboratively by sharing information, practices and policies to combat common cyber security challenges arising from the threat of ransomware.

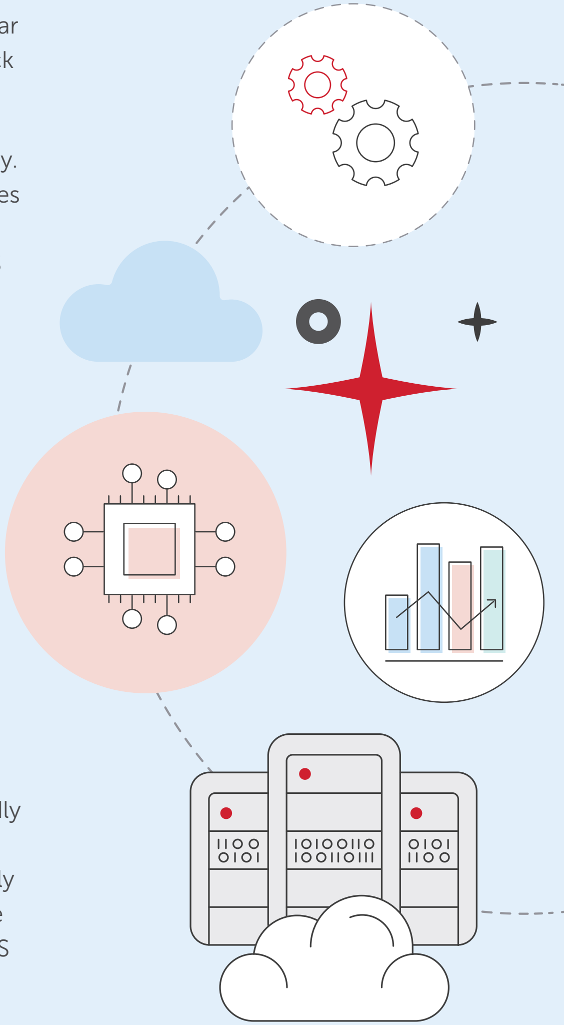
The ripple effects of a ransomware attack: JBS Foods

The ransomware attack on JBS Foods last year highlights the havoc that a ransomware attack can wreak on an organisation.

JBS Foods is global food processing company. It has 47 facilities across Australia and operates the largest network of product facilities and feedlots in the country. On 30 May 2021, JBS Foods suffered a ransomware attack that debilitated the company's operations in both Australia and the US.

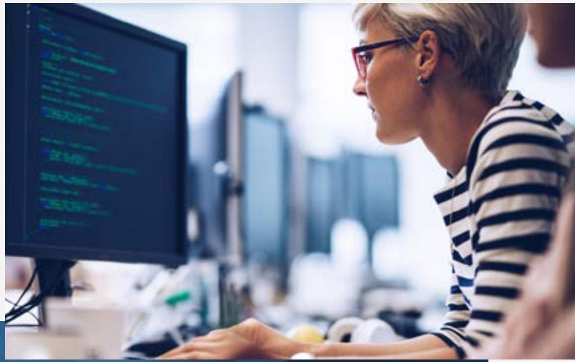
The attack led to a five-day shutdown of the company's Australian meat supply chain, the cancellation of livestock shipments and temporary lay-offs at some of the company's worksites. It has been reported that JBS Foods subsequently paid a ransom amount in excess of A$14 million.

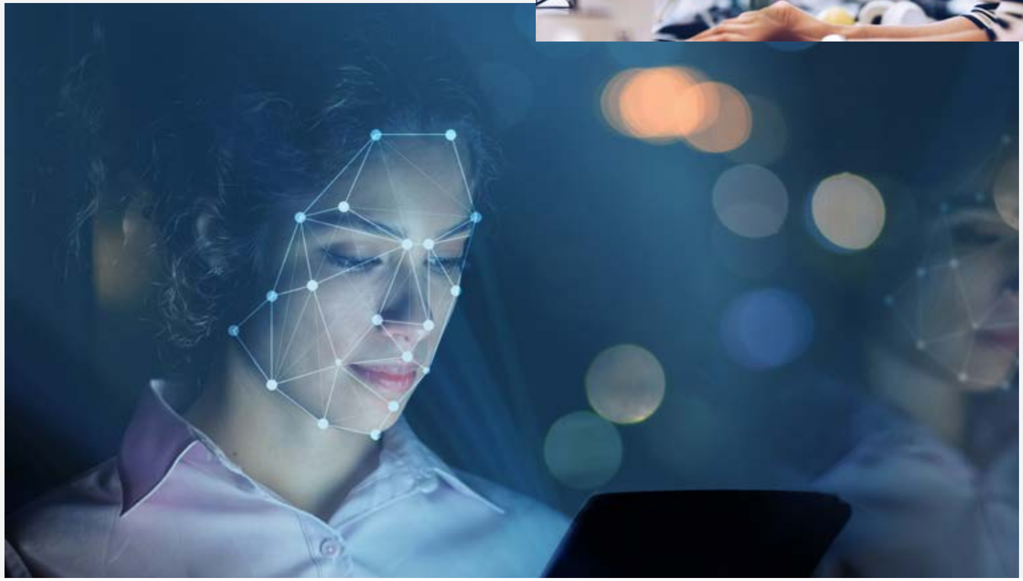
While the financial impact on JBS Foods was significant, the consequential effects on the community were also considerable. In Australia, JBS Foods' casual workers reportedly lost more than a week's worth of work and pay. In the US, rival meat producers reportedly raised beef wholesale prices as a result of the reduced supply caused by the absence of JBS Foods in the market.



Legal implications of paying a ransom

- There is currently no express prohibition under any Commonwealth, state or territory law that prohibits an organisation from paying a ransom amount in connection with a ransomware incident. However, the Australian Government's clear and stated position is that it does not condone ransom payments being made to cybercriminals.
- There are, however, criminal offences that may prohibit the payment of a ransom in circumstances where a person is reckless or negligent as to whether or not the money will become an instrument of crime. Depending on the circumstances of the incident, the defence of duress may be pleaded against these offences.
- In New South Wales, it is an offence, under the *Crimes Act 1900* (NSW), for a person to fail to report a serious indictable offence to the NSW Police where that person is in possession of information that will materially assist in apprehending, prosecuting or convicting an offender. The application of this offence is uncertain in the context of ransomware and other cyber attacks – particularly in circumstances where the malicious actor cannot be identified.
- Australian organisations and individuals who pay ransom amounts may be considered to have committed a criminal offence by breaching Commonwealth legislation that governs international sanctions regimes or criminalises the financing of terrorist organisations.
- Increased sanctions activity overseas may also be reflected in Australia's own regime. In the US, sanctions laws are strict and any US entity paying a ransom to a national of a listed region violates the sanctions prohibition. Non-US companies may also violate US sanctions if they cause a US person to violate the sanctions prohibitions.
- The risks of committing such offences may be mitigated by conducting due diligence on the organisation seeking the ransom payment, to confirm (to the extent possible) that it is not a terrorist or sanctioned organisation, or a known criminal syndicate. Where the defence of duress is available, the risk of committing an offence can be further mitigated by collecting contemporaneous evidence of any imminent threat that could not reasonably be rendered ineffective without paying the ransom. Such evidence may include communications with the malicious threat actors, providing evidence of exfiltrated data, and threats to release data or take other adverse action should the ransom demand not be paid.
- Victims of ransomware attacks should also consider their cyber insurance, and in particular whether payment of ransom is covered. For more information, see our discussion on pages 15 and 19 in relation to recent developments in the cyber insurance market.





Practical steps for Australian organisations

This section sets out key actions that that organisations should take arising from this year's research, survey and interviews. These steps should form part of an organisation's overall cyber resilience strategy.

1 Align cyber security measures with an external framework

Organisations should assess their cyber security maturity, and align it with external frameworks such as the ASD Essential Eight Maturity Model or the NIST Cybersecurity Framework.

They should also carefully focus on mitigating supply chain risk, by understanding what information is being held by third parties; by conducting appropriate due diligence on, and uplifting their contractual arrangements with, their key suppliers; and by actually exercising contractual audit rights where appropriate.

2 Conduct cyber incident response plan drills, regularly update plans and ensure that they are aligned to broader risk management

Organisations should regularly test their cyber incident response plans. While most organisations have developed tailored incident response plans, our survey indicates that only 59% are regularly testing and updating them.

The cyber risk landscape is changing rapidly – in light of new and onerous regulatory requirements; geopolitical influences; the accelerated adoption of new technologies; the rise in organisations' reliance on third-party suppliers; and the increase in the volume of malicious activity and sophistication of malicious actors.

Cyber incident response plans must be regularly tested and updated to reflect this fraught and ever-changing environment. Organisations should also consider developing and testing a ransomware-specific playbook, which should include escalations (including specific timing) and authority levels; and financial, regulatory, reputational and other factors to be considered in determining whether or not to make a payment.

In addition, organisations are collecting, creating and processing more data than ever. Boards and leaders must take concerted steps to understand the types of data their organisations hold and where this data may be exposed internally and externally across the supply chain. In doing so, the organisation will better understand genuine risk and exposure levels, and enable the application of a more focused cyber risk mitigation strategy.

Finally, organisations should also ensure that they are aligning their approach to cyber security and incident response planning with their broader organisational approach to risk, and are integrating their cyber incident response plans into their business resilience and crisis management strategies.

3 Train and educate employees, don’t underestimate the insider threat, and continue to invest in and improve security architecture

Human error still plays a key part in many (if not most) serious cyber incidents.

Employees – and in some cases customers – require appropriate and ongoing training and education to reinforce the importance of their roles in managing and protecting data and systems, and to enable them to identify and respond to cyber attacks.

Organisations should also implement policies and processes to assist them in quickly identifying and addressing insider threats. The risk and potential impact of these threats should not be underestimated.

Finally, organisations must continue to invest in and improve their security-related technologies and processes, including, for example, by:

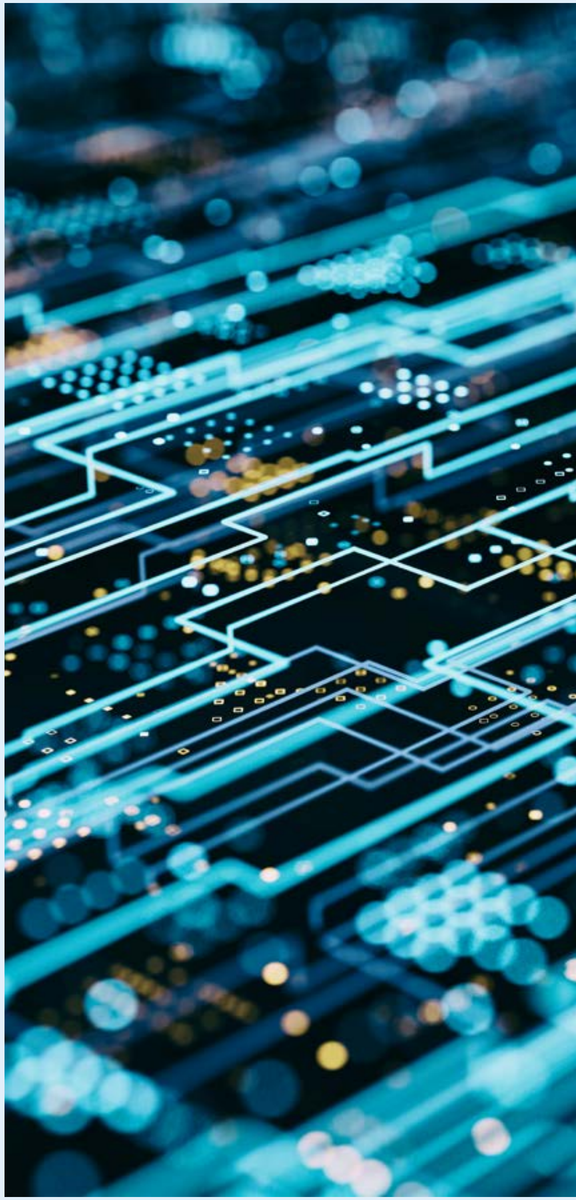
- applying best practice patching patterns;
- developing genuine capability for the timely decommissioning of out-of-support products;
- transitioning to a zero-trust model for mitigating risk arising from environment complexity;
- improving identity and authorisation hygiene by reducing the impact of poor end user decisions;
- integrating and harmonising monitoring capabilities to include behavioural outlier detection for administrative accounts, third-party vendors and end users; and
- uplifting confidence in, and the performance of, incident recovery systems.

4 Understand compliance obligations

Many organisations face an ever-increasing and more complex array of regulatory obligations – from notification requirements under the Privacy Act and the APRA Prudential Standards, to the new ASIC market integrity and SOCI laws. Many of these laws impose significant penalties for non-compliance.

In addition, as discussed on page 20, the Australian Government has foreshadowed plans to introduce new ransomware-specific laws, as well as conduct an overhaul of Australia’s privacy laws, which will include a substantial increase in the penalties under the Privacy Act.

Organisations need to urgently take steps to address new regulatory obligations imposed on them under the SOCI laws, and should also consider pre-emptively preparing for the likely imposition of new privacy and cyber-related regulation – including by identifying key data assets, and critically reviewing and updating their privacy and cyber-related policies, procedures and processes.



How we can help

MinterEllison provides a unique, full-service IT legal, risk and consulting practice, with extensive experience in privacy, data protection and IT sourcing and procurement.

Taking a pragmatic risk management approach, we work with senior management and Boards to implement frameworks to mitigate against cyber attacks. We also work with clients across the public and private sector to manage the full lifecycle of IT projects – from initial market approaches to contract negotiation to ongoing implementation and performance management. We bring deep industry experience, technical knowledge and legal expertise together to deliver the best possible outcomes for our clients.

- Procurement structuring and probity
- Software and ICT service procurement
- Digital transformations and outsourcing
- Incident response, breach coaching and crisis management
- Telecommunications regulation
- Privacy and data protection regulation
- IP protection and enforcement
- Investigative support
- IP commercialisation
- Dispute resolution
- Cyber risk Board governance
- Cyber risk and maturity assessment
- Strategic risk guidance and integration

PLAN

PROTECT

FORTIFY

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 their cyber resilience.

Paul Kallenbach
Partner
Competition, Risk & Regulatory

E paul.kallenbach@minterellison.com
P +61 3 8608 2622

minterellison.com

MinterEllison.