



15 February 2024

Conference Wrap: Insights from the Cyber Summit



Readiness



Response



Recovery

Opening address to the Summit



Make no mistake, cybercriminals are a remarkable adversary.

Among their ranks are pioneers: world-leading experts, visionaries in the tech space, leaders with exceptional foresight.

They are rich with resources, backed by investors and empowered by policymakers.

Their work touches the lives of millions, it spans all known borders and drives geopolitical change.

They exploit regulation, human emotion and commercial pressure effortlessly ... the strongest thrive and multiply.

It is this challenge which brings us together, that unites us behind the ambition of becoming the most cyber secure nation by 2030.

As a sector, we must determine a roadmap forward. We must find the opportunities within the Government's strategy to get us there.

We need to come together to build something irresistible, something that cybercriminals the world-over will fear.

Clyde & Co's ONE Cyber Summit came together on 15 February 2024 to find this alignment. To find the common ground and the rules of engagement needed to energise this journey forward.

Since the beginning, the cybersecurity and insurance industries have been at the heart of this fightback...very much part of turning the tide.

Similarly, the business sector isn't sitting idle. Boards have rightly made cybersecurity their number one priority, driving change.

Law enforcement agencies are stepping up, having disarmed some of the most prolific cyber gangs of their weapons.

Our government has implemented a first-of-its kind cyber sanction, unmasking a previously faceless criminal ... one of the biggest gangsters of our time.

Against international trends. Ransomware attacks here, are down. Payments are down. We must continue to install friction and deterrence into the cybercrime economy.

Business Email Compromise (**BEC**) and Funds Transfer Fraud (**FTF**) are still a problem.

We are writing half a billion dollars in cheques to cyber gangs every year.

Third-party breaches and supply chain attacks continue to dominate. We've seen ports shut and supply chains shudder.

Small businesses continue to battle – to defend against a threat that could end their operations with the click of a mouse.

So what is the answer?

We must think differently – **together**.

If we are to become the most cyber secure nation ... we must unite.

We must be stronger – **together**.

On behalf of the entire team, thank you for your support.

To those who attended the Summit, and to those that couldn't make it, we look forward to joining in this mission with you.

Contents

Opening address to the Summit	2
Foreword: Stronger Together	4
The Cyber Shields	6
Summary of key findings	7
Keynote opener and acknowledgements	8
Shield 1: Strong Business and Citizens/ Shield 2: Safe technology	10
Unity against cyber crime: bringing industry together to boost cyber resilience	10
Stories from the frontline: navigating third-party service provider incidents	12
OAIC Privacy Commissioner fireside discussion	14
Shield 3: Threat Sharing and Blocking	15
Rethinking industry-government collaboration in the wake of a cyber incident	15
Shield 4: Protected critical infrastructure	18
Lighting the way forward: safeguarding critical infrastructure in the digital age	18
Cyber incident notification strategy, crisis communications and reputation management	20
Shield 5: Sovereign capabilities/ Shield 6: Resilient region and global leadership	23
The road ahead: becoming a world leader in cybersecurity by 2030	23
Key audience takeaways from the day	25
Under The Hood – Key findings	30
Our Summit Partners	33
Authors	40

Stronger Together: Embracing Strategy and Shields on the road to a more Cyber Secure 2030

We've seen significant change across the cybersecurity sector since our inaugural Cyber Summit in May 2023 – most notably the Federal Government's increased capacity to address cyber risk nationwide, at all levels.

Underpinning this development is the Cybersecurity Strategy (**the Strategy**) and Action Plan released by the Government late last year, and its current Consultation Paper which looks towards potential new laws and reporting mechanisms.

On exhibition until March 2024, the outcome of this process could have significant and wide-ranging implications for the cyber industry and how businesses protect against and respond to cyber incidents in the future.

In response to this shifting landscape, we brought our clients, regulators, government and the cybersecurity and insurance industries together to unpack how this strategy combined with potential regulatory change could help pave the way to establishing Australia as the most cyber secure nation by 2030.







Our mission: to bring together the difference makers to enable change.

John Moran, Reece Corbett-Wilkins, Richard Berkahn, Stefanie Luhrs, Alec Christie, Chris McLaughlin, Richard Martin, Andrew Brewer and the rest of the team.



The Cyber Shields

Under the Federal Government's Cyber Security Strategy sit six 'cyber shields' which set out the main areas of focus in addressing the nation's cyber resilience moving forward.

 <p>1</p> <p>Strong business and citizens – our businesses and citizens are better protected from cyber threats and are more equipped to recover quickly in the event of a cyber-attack.</p>	 <p>2</p> <p>Safe technology – we can trust that our digital products and services are safe, secure and fit for purpose.</p>	 <p>3</p> <p>World-class threat sharing and blocking – we have real-time threat data, and we can block threats at scale.</p>
 <p>4</p> <p>Protected critical infrastructure – our essential services can withstand and bounce back from cyber-attacks.</p>	 <p>5</p> <p>Sovereign capabilities – we have a flourishing cyber industry with a diverse cyber workforce.</p>	 <p>6</p> <p>Resilient region and global leadership – our region is more cyber resilient and will prosper from the digital economy. We will continue to uphold international law while shaping global rules and standards in line with shared interests.</p>

Using the shields to inspire our Summit agenda, we focused an investigative lens over these goalposts and how they can help drive positive change, while also addressing the potential downfalls and difficulties that could be faced along the way.

Expert speakers were hand-selected for the day, to bring their experience and views to the audience. We thank the speakers for their contribution to the discussion on the day.

Summary of key findings:

In working **Stronger Together** the key themes of the day were:

- 1**

Cyber insurance – The global cyber insurance industry is actively supporting clients uplift their cybersecurity controls and incident response capabilities. There is an opportunity for Government to work with insurers and brokers at an aggregate level, and to promote the uptake of cyber insurance particularly for SMEs.
- 2**

Information sharing – The private sector, incident response industry and Government have an opportunity to develop a world leading threat sharing capability pre, during and post breach. However clear rules of engagement and legal protections need to be in place to work most effectively.
- 3**

Small business focus – We are a nation of small businesses. Free resources, centralised reporting frameworks, and playbooks will help reduce compliance burden. However financially incentivising small business uplift should be considered, as well as harnessing the trickle-down effect of broad security frameworks (e.g. SOCI) across all supply chains to lift the bottom line.
- 4**

Third-party breaches – Multi party data breaches often grip entire industries at once. Parties involved in breach response have an opportunity to work better together under a common goal to manage consequences. More work can be done pre-breach in setting expectations, roles, and responsibilities.
- 5**

Team effort – Within organisations, there continues to be an opportunity for cyber risk to be approached on a multi-disciplinary basis with representatives from Legal, IT, Risk, Insurance, Comms, and Boards taking an active interest. Government can use this to drive skilled migration policies and continue to build a diverse workforce across technical and non-technical disciplines.

Keynote opener

We were delighted to welcome the then Acting National Cybersecurity Coordinator, **Hamish Hansford**, to kick off our Summit with an overview of the new Cyber Security Strategy and Action Plan, current Consultation Paper, and to provide insight into the work the Government is undertaking behind the scenes to tackle cybercrime.

At the forefront of leading the ongoing uplift in the critical infrastructure sector, Hamish has led the Government's response to some of our nation's largest and most complex security incidents. Additionally, his team have been very busy over the last 12 months – hosting 50 consultation events on the Strategy, considering over 330 submissions, co-designing the Strategy itself, and more recently engaging with businesses on the roll out.

During his keynote speech, the Acting National Cybersecurity Coordinator addressed the wholesale changes the Government is looking to introduce – with the aim of building resilience and longevity into our country's broader cybersecurity posture.

The key takeaway was that Government is focussing their efforts on addressing cyber risk at the aggregate level – including addressing 'safe technology' to protect consumers, businesses and enhancing 'information sharing' to enable businesses to better understand and manage cyber risks, and Government to better respond to the cybercrime threat.

Acknowledgements

A reoccurring theme throughout the Summit was the importance of resilience – individually, collectively, and as a nation.

We were incredibly fortunate to also hear from three individuals who could speak about the power of this force from their own individual experiences.

In delivering a Welcome to Country, Dharawal woman and Indigenous Elder **Aunty Maxine Ryan** spoke of the resilience that First Nations people continue to draw on to both safeguard and share the culture and heritage of the Traditional Custodians of the land.

Paralympian **Annabelle Williams OAM** captivated the room as she spoke of those people throughout her life who had instilled in her the resilience that would drive her to a gold medal at the 2012 London games.

Finally **Professor Arnold Dix** combined evocative storytelling with some dramatic sound and visuals to talk for the first time about his part in the lifesaving rescue of 41 Indian workers trapped in a collapsed tunnel in the Himalayas – and the strength of determination that helped drive him forward.

We wish to thank each speaker for their part in the 2024 Summit.





Shield 1: **Strong business and citizens** and
Shield 2: **Safe technology**

Unity against cybercrime

Bringing industry together to boost cyber resilience

As implied by the first shield, building strong cyber resilience in businesses of all sizes across the country is one of the biggest challenges we as a nation face. To help us explore this area further, we brought together representatives from large corporates, small business, government, and the insurance sector to discuss the potential opportunities and difficulties with creating a unified approach to cybersecurity and incident response.

Featuring **John Moran** (Partner at Clyde & Co), **Christian Gergis** (Head of Policy at the Australian Institute of Company Directors (AICD)), **Andrew Hall** (CEO of the Insurance Council of Australia (ICA)), **Jamie Wilson** (Consulting member of the Small Business Association of Australia), and **Anna Johnston** (ex Deputy Privacy Commissioner of NSW and consultant to government at Salinger Privacy), this session examined how industry, insurance and government all play a critical role in helping Australia collectively understand cyber risk and can, by extension, boost cyber resilience.

Key takeaways from the Unity against cyber crime session included:

- Cyber resilience must be built from the ground up. Panel members agreed that this means having sound foundational processes as well as ensuring that Australians (individuals and businesses) can trust their digital products and software.
- The cyber resilience of small-medium enterprises (SMEs) is a key piece to Australia's cyber resilience as a whole, especially given we are a nation of small businesses.
- Government and the insurance industry play a critical role in providing access to tools to measure cyber risk and education to uplift the cybersecurity

posture of SMEs to ensure that they are prepared for cybersecurity attacks and incidents.

- There are free tools and guides available from government and industry providing very cost-effective entries to lowering cyber and associated legal risk. The AICD specifically mentioned their upcoming report which has since been released providing guidance to Directors and Officers on how to approach cyber risk across Readiness, Response, Recovery and Remediation lenses.

[\[https://www.aicd.com.au/risk-management/framework/cyber-security/governing-through-a-cyber-crisis.html\]](https://www.aicd.com.au/risk-management/framework/cyber-security/governing-through-a-cyber-crisis.html)

- The insurance industry not only has an important role in uplifting the security controls and processes for policyholders, but also plays a crucial role in the response to a cyber incident by making it easier for Australian business to access advice and support post-breach.
- The proposed changes to the Privacy Act are expected to provide further clarity on privacy obligations for Australian businesses, but also means that there may be emerging regulatory risks, particularly for SMEs.
- Cyber risk is far-reaching and can present in the form of third-party claims, representative actions, shareholder class actions and regulatory actions. The insurance industry is headed in a positive direction and is well placed to provide more holistic cover for these risks.

Total ransomware payouts reached \$1.1 billion USD globally in 2023

Source: Chainalysis Report 2024



Stories from the frontline

Navigating third-party service provider incidents

Despite best efforts to invest in cybersecurity, we know that organisations are only as strong as the weakest link in their supply chain. Threat actors understand that by targeting a single third-party vendor, they can simultaneously impact multiple organisations with minimal effort.

Richard Berkahn (Partner at Clyde & Co) delved into the risks presented by a third-party supplier incident and explored the firsthand experiences of some entities who faced the task of responding to another party's breach.

Catherine Harding (Chief Operating Officer at Australia for UNHCR), **Dane Mitchell** (Managing Director at Optimum Allied Health), and **Anna Golovsky** (Executive Manager for Legal Operations at IAG) shared their insights and key lessons learned.

Key takeaways from the Stories from the frontline included:

- The panel underscored the importance of proactive cyber risk mitigation, with cyber insurance playing a crucial role in enhancing organisational resilience and response efforts.
- The panelists each explored their own experience of the benefits of a well-prepared team, including having a robust incident response plan (IRP) and conducting regular scenario testing involving third-party providers.
- The panel explored the unique challenges of managing responses to third-party incidents, including constrained information flow, limited control over affected systems, dependency on suppliers for critical services, and complex regulatory compliance.
- Following their experience of a third-party breach, the panel recommended entities conduct regular reviews of security practices across their supply chain and set clear expectations for their third-party providers, particularly regarding data retention and disposal. The respective incidents experienced by each panelist reinforced the importance of revisiting existing data sharing arrangements with suppliers to ensure accurate visibility over data risk.
- Representing the views of small businesses, the panel stressed the need for organisations, especially SMEs, to have a greater awareness of the significant regulatory and financial risks posed by cyber incidents, drawing lessons from others who have been there before. Generally, it was felt that SMEs are unaware of the true extent of cyber and data privacy risk, until they had experienced an incident.

- Consensus was reached on the value of cyber insurance in providing financial protection and ensuring regulatory compliance. The panel also noted that insurers often require policyholders to adhere to strict security standards, thereby bolstering overall cybersecurity posture. While the process of obtaining insurance can be cumbersome, it should be seen as an investment in ensuring that security controls and processes are in line with best practice and reflective of the current threat landscape.
- The panel agreed that further discussion is warranted on the merits of mandating cyber insurance for organisations handling high-risk or large volumes of data – and that the Government should look at this for certain industries, or parties should mandate it in their contracts with their supply chain. This will ensure that as many companies as possible have the financial means to adequately respond to cyber incidents.

An incident is reported every 6 minutes in Australia to the ACSC through ReportCyber

(Source: ACSC 2023 Threat Report)



OAIC Privacy Commissioner fireside discussion

To help us further understand Government expectations around protecting individuals affected by a cyber incident, we heard first-hand from the Office of the Australian Information Commissioner (OAIC) Privacy Commissioner **Angelene Falk** who delved into the Notifiable Data Breaches Scheme and its impact since it was first introduced six years ago.

The Privacy Commissioner emphasised the important of having prevention strategies and ready-to-go response plans in place which are critical to reducing risk of serious harm, and that OAIC's upcoming report will break down the big trends they've seen in cyber incidents over the last six months. Following the Summit, the latest NDB Report has been published and is available online.

Commissioner Falk also provided insights into the OAIC's enforcement priorities for 2024, including the review of the Privacy Act 1988 (**Privacy Act**), and detailed the proactive steps the OAIC are taking to reduce the risk of harm to citizens from future cyber-attacks.

<https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-july-to-december-2023>



Shield 3: Threat sharing and blocking

In trust we share

Rethinking industry-government collaboration in the wake of a cyber incident

A reoccurring theme throughout the day was the need for government and industry to work together to face down cyber crime.

Stefanie Luhrs (Partner at Clyde & Co) led an expert discussion on how this relationship is evolving, with expert insights from **Rob Champion** (Queensland Government CISO), **Ian Birdsey** (UK Partner at Clyde & Co), **Philip Heuzenroeder** (IPH Ltd General Counsel), and **Olga Ganopolsky** (Macquarie Bank General Counsel – Privacy and Data).

Key takeaways from the In trust we share panel included:

- Industry engagement with government threat intelligence initiatives is for the collective good, and critical to identifying and mitigating vulnerabilities at national level.
- The panel discussed three key proposals in the Cyber Strategy, aimed at promoting greater public-private collaboration with regards to cyber incident information-sharing, including:
 - implementing a 'limited use' information sharing obligation (for prescribed cybersecurity purposes);
 - implementing a no-fault, no-liability ransomware reporting obligation; and
 - establishing a Cyber Incident Review Board to conduct no-fault post-incident reviews.
- The panel generally agreed that there is a need to bridge the gap between government information requests and industry reluctance to cooperate, however, noted organisations are cautious and have reservations about sharing sensitive information that could potentially be used against them later.
- Drawing on his expertise, Clyde & Co's Ian Birdsey shared positive examples of information sharing in the UK, highlighting that when done well, it can be mutually beneficial for all parties. Ian balanced these examples by providing insights to the complexities of privileged communications, emphasising the importance of maintaining transparency while safeguarding against self-incrimination.
- The panel also reflected on the practical impacts of receiving information requests from various agencies in a live incident

context, noting that the response process can be onerous and distracting, especially when the incident is high-risk, time-sensitive or rapidly-evolving.

- The panel agreed that information-sharing initiatives must strike a delicate balance between both practicality and real-world impacts, and ultimately intelligence should be actionable.
- Sharing insights from an international perspective, Ian spoke to the UK's clear delineation between information-sharing with government and regulators while others reflected on lessons learned from success stories closer to home, such as the Optus and Medibank incidents.
- Overall, the panel were in favour of public and private sector information sharing models, however cautioned against the need to balance various competing stakeholder interests.



Willingness to pay ransoms has dropped from 85% in 2019 to 29% in 2023

Source: Coveware Report 2024



Lighting the way forward

Safeguarding critical infrastructure in the digital age

Cybercriminals are rapidly adjusting their technology, techniques, and tactics to exploit any weakness they can find.

Those working on the frontline of this digital battleground have their work cut out – particularly those responsible for protecting our critical systems and infrastructure.

In this session, **Alec Christie** (Partner at Clyde & Co) explored the many complexities of risk facing critical infrastructure entities with expert panellists **Sophie Mitchell** (.auDA Chief Communications Officer), **Matt Lange** (APA General Manager Enterprise Security), and **Sally Pfeiffer** (Home Affairs First Assistant Secretary), sharing their thoughts on the prevailing legislative framework and the challenges ahead.

Key takeaways from the Lighting the way forward panel included:

- *Security of Critical Infrastructure Act 2018 (Cth) ('SOCI')* is one of the most significant, important and uplifting cybersecurity laws – yet many are unaware of its application, operation and obligations.
- SOCI imposes positive obligations on 11 classes with 22 (and possibly further) critical infrastructure assets. However, obligations are not activated for all critical infrastructure assets.
- Panellists commented that compliance can be complex – not only must you determine whether your assets fall within SOCI's criteria, but you must

understand the components of your assets. Despite the complexity, there was agreement across the panel that it has solidified security risks practices leading to greater understanding and management of the business risks.

- The critical infrastructure risk management program is the heart and soul of SOCI. The concept of a risk management plan is not new. However, under SOCI, the “program” is about the plan and program of activities in place to mitigate material risks against certain hazard domains. This can be of assistance to anybody – not just critical infrastructure. If it works for critical infrastructure, we can expect these obligations to rolled out more widely.

- Additionally, the panel noted that even if you aren't directly caught by SOCI obligations, one of your customers might be. You could be a key provider, supplier or data centre with a contract with a SOCI entity. In a supply chain context, it's very easy to get “caught in the net” (e.g., a responsible entity may want to pass SOCI obligations on to its supply chain).
- There were some useful action items provided by the panel – join your TISN and get involved, implement ASD Essential 8, understand your assets and if they captured by SOCI criteria, interpret components, and implement a risk management program.

Critical infrastructure attacks increased by 50% in 2023

Source: Australian Signals Directorate, ACSC Report



A shifting story

Cyber incident notification strategy, crisis communications and reputation management

While a cyber-attack on any of our critical infrastructure would certainly make headlines, the general response from media, the public, shareholders, and even impacted individuals to a cyber incident is shifting.

As people become more aware of such incidents, a prevailing perception becomes entrenched. In some ways, that provides a basis from which to shape a narrative, but it also introduces misconceptions, misunderstandings and myths.

With the reaction to cyber incidents evolving, Clyde & Co's Director of Cyber Communications **Richard Martin** invited **Sean Berry** (former advisor to the NSW Government during COVID) **Commissioner Rob Rogers** (NSW Rural Fire Service), and **Professor Cassandra Cross** (Queensland University of Technology School of Justice) to discuss the ever-shifting landscape of communicating in a crisis.

Key takeaways from the A shifting story panel included:

- Technology is driving change at an exceptional rate. Historically, communications focused on what has happened – today's 24 hour news agenda moves at such a pace that the need to forward think, provide instant updates and lead the narrative is acute.
- The prevalence of information sources has made the task of meeting and supporting the victims of crime or those facing disasters much harder, with resonate content drowned out by counter narrative and sensational reporting.
- Language choice in statements underscores the importance of precise and inclusive messaging while incorporating a human element into responses is also advantageous to drive the narrative effectively.
- Timely and transparent data notification or communications, particularly when sharing negative news, is important to foster trust and transparency throughout an incident.
- Balancing transparency with empathy in communications strategies is essential, as is organisations taking ownership of their responsibilities, which tends to lead to a more positive response from stakeholders.
- Tailoring communications approaches to diverse communities and socio-economic backgrounds ensures widespread understanding and engagement.
- Overall, embracing open conversations, leveraging technology, and recognising the importance of media can contribute to more effective communications during incidents.



The average loss for a BEC funds misdirection is more than AUD \$100,000

Source: Clyde & Co Whitepaper 2024



Over 90% of BEC and ransomware incidents impact small to medium businesses

Source: Clyde & Co Whitepaper 2024



Shield 5: **Sovereign capabilities** and Shield 6: **Resilient region and global leadership**

The road ahead

Becoming a world leader in cybersecurity by 2030

After hearing about the Strategy and associated actions/plans, it was important to discern the work going on behind the scenes to uplift our national workforce, and what steps are being taken to make Australia a harder target for cybercriminals.

Richard Berkahn (Partner at Clyde & Co) was joined by **Hugh Watson** (Department of Foreign Affairs and Trade (DFAT)), **James Baker** (Australian Cybersecurity Centre (ACSC)), **Assistant Commissioner Scott Lee** (Australian Federal Police (AFP)), and **Joe Smith** (Cyber Security Response Coordination Unit (CSRCU), Home Affairs) to share their insights and thoughts on where we can end up as a nation operating within a complex regional and global geo-political environment.

Key takeaways from the The road ahead panel included:

- Government wants to attract, recruit and retain cybersecurity professionals either through domestic, international (migration) or government means. There's also a push on how to identify and integrate generalists in the cyber space and how their skills can be recognised.
- Utilising the Five Eyes alliance, as well as international law enforcement such as Europol, will strengthen capability within the APAC region. These collective efforts have been essential in increasing Australia's protection from cybercrime.
- A key strategy to prevent, deter and respond to cyber crime is through the naming and shaming of cybercriminals, or nation states. This is important to show cybercriminals that Australia is a hard target and that we have the tools to reveal identities.
- All panellists stressed the importance and heavy reliance that Government has on industry partners to address and prevent incidents.
- Government is keen for organisations to report ransomware incidents, even if they have paid a ransom to decrease victimisation of companies who have already fallen victim to an attack.

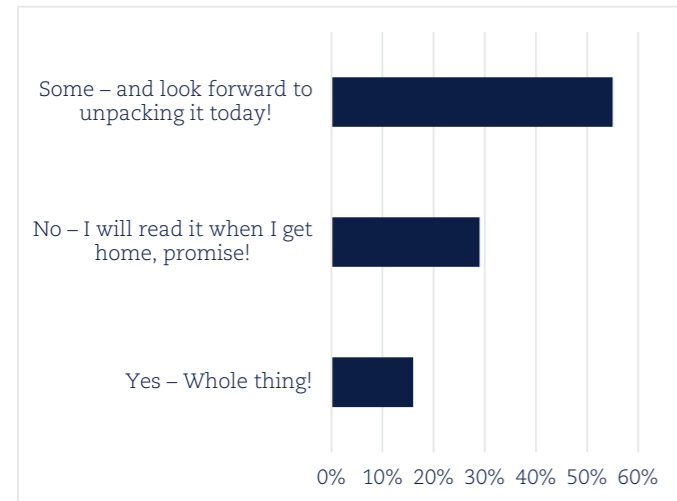
Key audience takeaways from the day

We must unite behind a common goal

There is a growing awareness among Australian decision-makers of the true impact of cybercrime. The question is how to direct that awareness into tangible advances when it comes to Australia's defences.

The Strategy can act as a roadmap, but delivery must be achieved in partnership: business, the public sector, the insurance sector and legal all having to take a shared ownership of its goals.

Have you read the Cybersecurity Strategy?



The audience were able to use the Summit to build upon their understanding of the Strategy and identify areas where they can contribute to its goals. This includes:

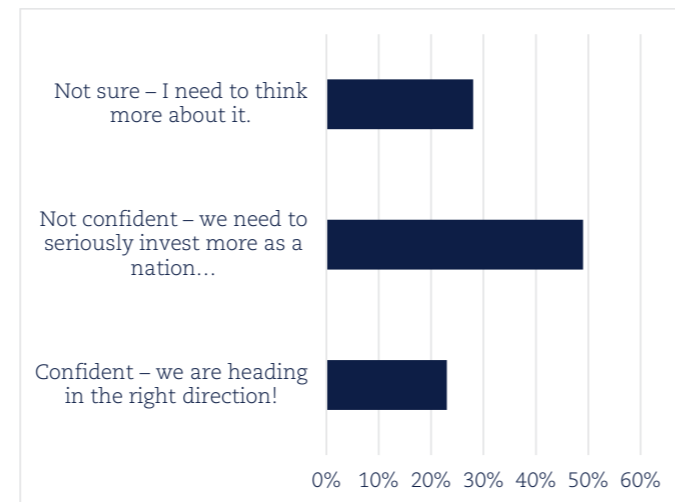
- engaging in key proposed law reforms (ransomware reporting, standalone Cybersecurity Act, SOCI);
- contributing to discussions on safe technology and threat sharing; and
- understanding our direction as a nation – our sovereign capabilities and our commitment to uplifting the region.

We must put our money where our mouth is

Ambition is not enough.

We must invest in the technology, the skills and the infrastructure that can meet with the determination to hold a role as a world leader in the cybersecurity space.

How confident are you that Australia will become the most cyber secure nation by 2030?



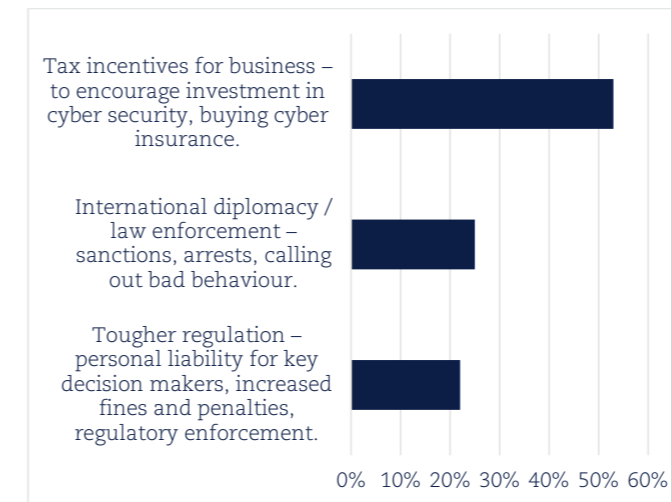
While public funding is both welcomed and anticipated, it must be met with additional resources from across the Australian economy in the form of investment in cyber readiness, response and recovery capabilities. Critically, this includes boosting the uptake of cyber insurance across the business sector (and particularly for SMEs) to ensure that the economy can withstand the costs of cyber crime and enable wholesale uplift of cybersecurity practices.

No one sector alone can fuel the journey towards 2030 – and no one entity can deliver the resources that are needed to secure market confidence that we are heading in the right direction. Only by working together, will we be able to move the dial on cyber risk.

Where government can play a leading role

To secure the increased resourcing which is crucial to Australia's ambition of becoming the most cyber secure nation, Government has a suite of options available to it. The audience reflected on where it thought Government can take steps to drive down cyber risk on a wholesale basis.

What is the most effective way for Government to reduce cyber-attacks?



Subsidising the costs of cybersecurity and purchasing cyber insurance is just one example of incentives for business to work towards becoming cyber secure.

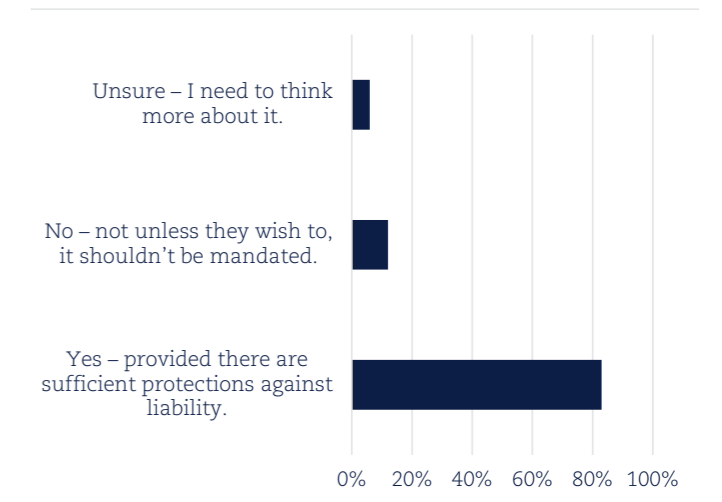
Rewarding those who are willing to invest in additional cyber resilience will encourage intentions to turn into actions, which collectively will help secure the country's IT environment as a whole.

Cyber risk is a shared community risk, and it takes a community approach to protect the nation.

Intelligence information as an asset

A united response requires greater sharing of data, insight and experience – between Government and industry. To facilitate that, big decisions need to be made in terms of the rules of engagement and delineation between public sector support, and regulatory oversight.

Should organisations be required to share information about ransomware attacks with the government?



To harness effective collaboration and achieve the culture of transparency we are working towards, businesses need to be confident that there are protections against liability. Without this assurance, there will always be reluctance to share information and learnings.

This interplay must be governed by trust, driven by information-sharing initiatives that span both the practical, and the pragmatic. As this interplay gathers pace, the opportunity will meet with the ambition – creating a valuable source of intelligence that threat actors will be unable to match.

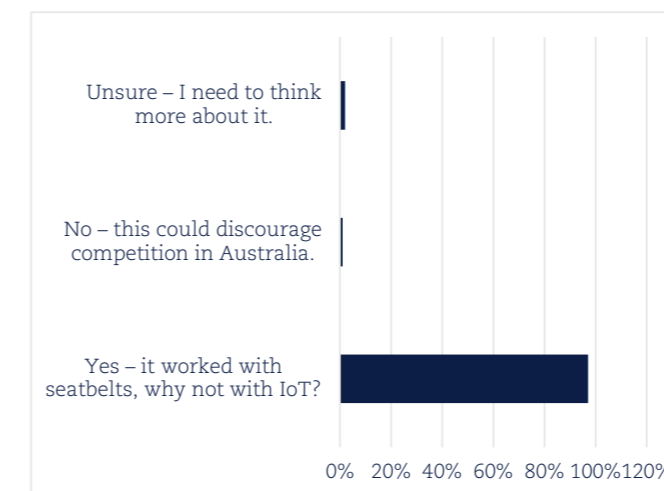


Safe technology – safe communities

In building safer communities, technology providers have a clear duty to ensure that their products and services have cyber safety at their core.

There is resounding support for increasing the standards on technology providers – international standards, stronger data retention obligations and the embedding of cybersecurity into emerging technologies are all part of the way forward.

Should we impose minimum security standards on technology providers?

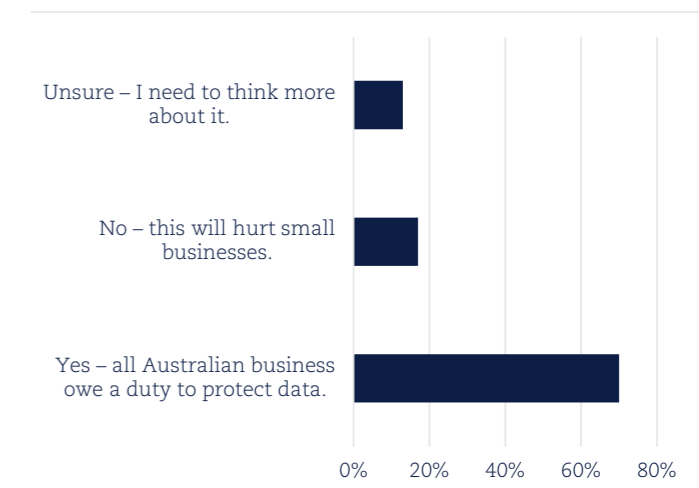


As with seat belts, imposing action may be resented by the few, but will benefit the many. The audience was strong in their support for such wholesale reform.

We're in this together

While alive to the pressures on small business, a cyber secure Australia must rely on all parts of the economy in order to meet its goals. Investment must be expected to align with capability, but it must also be expected across the board. In a nation of small businesses, their role in securing the ambitions of the Strategy are crucial.

Should we remove the Small Business Exemption in the Privacy Act?

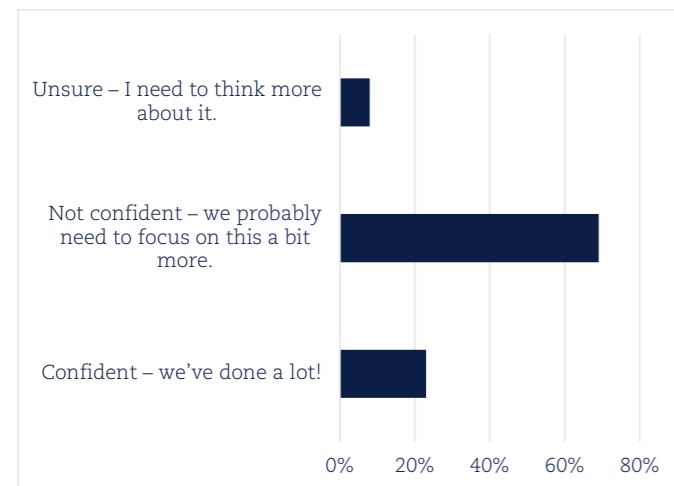


With that said, compliance with the Privacy Act comes at significant cost – the government recognises this and will be implementing various initiatives before broadening the scope of its application.

Supply chain risk remains a concern

An increasingly interconnected economy will rely on the seamless exchange of data between organisations, but the pace of change is building vulnerability into the heart of this evolution. When responsibility becomes a shared obligation, parties must surrender some control and place their fate at least partially in the hands of others.

How confident are you in managing your supply chain / third party cyber risks?

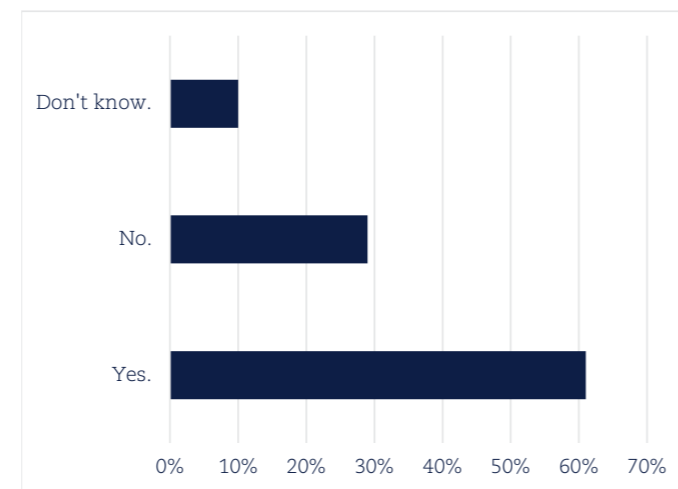


Solid rules of engagement, clear regulation and minimum security standards will provide additional confidence for organisations entering into such interactions – allowing cybersecurity to grow alongside economic opportunity.

No third-party incident? You're in the minority

The well-worn adage goes that 'it's not a case of if, rather when' you will face a cyber incident. When that likelihood is applied across your partner organisations and suppliers, the threat facing Australian business is brought into focus.

Has your organisation ever been impacted by a third-party incident?



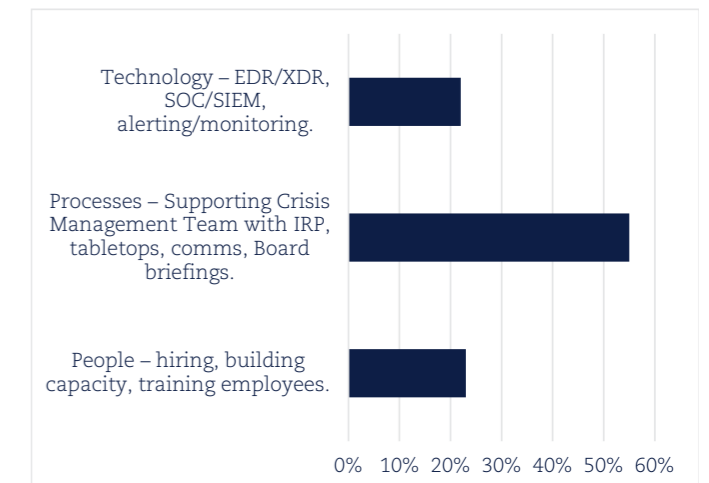
A greater investment needs to be directed towards empowering a combined response to these incidents, allowing for the additional complexity that comes from coordinating engagement and balancing the conflicting needs of different groups of stakeholders.



Enhancing processes a top priority for 2024 (alongside people and technology)

While there are clearly supporters of a number approaches to building resilience over the coming year, it seems that streamlining plans and road testing playbooks will be a key activity for the sector.

Where are you focusing on in 2024?



Such thinking stands as a testament to the hard work completed over the past twelve months in terms of preparedness, and marks an increasing maturity in Australia's ability to respond to incidents when they emerge.

Under the Hood: Key findings

We also launched our white paper at the Summit - providing key findings and actionable data to support industry-wide initiatives and inform policy setting.

Key findings

We're heading in the right direction with ransomware



Return of 'big game hunting', rise in ransom demand quantum, despite record low ransom payment rates.



Threat actor fragmentation: spike in the utilisation of the RaaS business model. LockBit and BlackCat/ AlphVM most active RaaS groups observed.



Increase in data theft extortion only events. Data leaking the most prevalent double extortion tactic (44% of all ransomware incidents).

Business Email Compromise (BEC) incident losses demand equal priority alongside anti-ransomware initiatives



BEC and FTF collectively represent the bulk of incidents observed during the Analysis Period (making up 44% of all incidents observed).



Our economy continues to lose significant capital each year to BEC incidents and FTF. We know these losses typically have slim prospects of recovery if not caught quickly.



Human error, MFA bypass and failure of call back procedures top root cause.

Third-party breaches are the new ransomware



Ransomware was the number one cause of third-party breaches, accounting for 100% of these types of incidents occurring between **1 January 2022** through to **31 March 2023** (the **Analysis Period**)



Managed service providers (**MSPs**) are often the weak link – MSP breaches accounted for 42.85% of all third-party data breaches in the Analysis Period.

Small business, big challenge



Our data shows that small to medium sized incidents are where the volume of cyber incidents rest.



Of those matters analysed for the purpose of this report, **93% of BEC incidents** and **96% of ransomware incidents** impacted small or medium businesses.

The road ahead – where to focus your energy in 2024

In the Guide, we identify the top items that we think make a real difference to the battle against cybercriminals and better prepare your organisation to decisively respond to cyber-attacks. Feel free to use this list as a guide on what to focus on in 2024.

We have summarised the key points below.

Get to know your incident response partners and processes

- build your incident response bench and introduce your external team to each other, clearly establish roles and responsibilities;
- identify which vendor will manage which incident response 'workstream', including IT containment and forensics, legal/regulatory advice, communications and Threat actor management; and
- contact your broker to organise a complimentary 'meet the breach coach' session to map out the process for activating the breach response service which sits behind the insurance policy (entirely separate from making an insurance claim).

Control and process uplift and remediation

- FTF – reinvestigate MFA and call back procedures for financial controllers' systems;

- supply chain risk management – uplift and test capabilities of third parties that jointly hold data or have administrative access to systems. Ensure alignment on how organisations will jointly assess, mitigate and notify data breaches; and
- counter-ransomware measures – keep on top of the latest exploited vulnerabilities, system access trends, and implement enhanced detection and response capabilities.

Effective data management

- **data audit** – review the types of data you hold, where it is held and by who, how long you have held it for, whether it is structured or unstructured, and whether there are adequate controls in place to protect it;
- **data retention / deletion / classification** – assess your legal obligations regarding the retention of data, develop a clear and workable framework to continuously review data management, consider better ways to store data (especially if it is not in active use). Where possible, delete data that is not required; and
- **training** – empower employees with effective data management training.

Train and test your IRP, CMT and Board

We highly recommend the crisis management team (CMT) (or equivalent) conduct at least one cyber readiness exercise per year.

Our Summit partners

We want to keep this Summit free for attendees and cannot do so without the continued support of the industry. The sponsors that attended and presented on the day understand the power of togetherness, and we acknowledge their support on an ongoing basis with this mission.

PLATINUM



Gridware

Gridware is a leading provider of Full-Spectrum Cybersecurity Services in Australia. Founded and based in Sydney, Gridware has quickly gained the trust of organisations becoming a critical partner to insurance providers to respond to cyber-attacks out of our 24/7 Cyber Defence Centre. Our vision is to make Australia the safest country in the world to do business on-line.

We provide earlier warning of more threats and respond with more solutions for more businesses while staying ahead of cybercriminals with deeper local expertise.

Our distinctive benefits include:

- Australian owned, operated with no off-shoring of talent
- Vendor Agnostic - the right tool for the right problem at the right budget at the right time
- Early-Warning - We've developed unique, proprietary early-warning dark web tools and other cyber innovations
- Deep insurance Industry expertise
- CREST Approved
- Flexible, Responsive and adaptable to customer needs
- Full-Spectrum, end-to-end cybersecurity solutions

P: 1300 211 235

E: info@gridware.com.au

W: <https://www.gridware.com.au/>

- Tabletop Exercise – a discussion-based exercise, an informal operational environment for team members to build their understanding of the incident response process;
- Cyber Simulation – hypothetical cyber incident in semi-real time to develop muscle memory and practice effective response using the actual structure of the CMT; and
- Cyber Fire Drill – an extended Simulation exercise (performed over the course of 2-5 days) with groups simultaneously working through the response at all levels.

2.5 Communications playbook

Crisis communications should cover everything from media management, social media engagement, staff communications, regulatory notifications, customer support, and ASX disclosure and government relations (where relevant). The focus is not just on what, when and how to say things, and to whom, but also thinking about how you would work with:

- government agencies on incidents with a national significance or where significant consumer redress support is required to mitigate harm to affected individuals;
- third parties where jointly held personal information is involved; and
- regulators and other agencies where reporting obligations are triggered.

Download the Guide

Please download a copy of our **Under the Hood Guide** or email us at **OneCyberSummit@clydeco.com** to obtain a copy of the summary presentation which you can use for internal discussions.



<https://sites-clydeco.vuturevx.com/304/18949/landing-pages/report-download-form-.asp>





McGrathNicol

McGrathNicol/ SentinelOne/ KELA

McGrathNicol is a specialist Advisory and Restructuring firm committed to helping businesses, large and small, to perform at their best, manage risk, and achieve stability and growth. McGrathNicol Advisory specialises in Cyber, Deals, Forensic, Government Advisory, Managing Risk and Strategy & Performance.

Our Cyber experts are committed to making Australia a hard target for cybercriminals. We offer cyber solutions to solve any scenario – from reducing risk, to recovery from a cyber incident and strategies to increasing your organisation’s resilience.

SentinelOne

SentinelOne is a leading provider of autonomous security solutions for endpoint, cloud, and identity environments. Revolutionising endpoint protection with a new AI-powered approach, our platform unifies prevention, detection, response, remediation, and forensics in a single, easy-to-use solution.

KELA

KELA Cyber Threat Intelligence provides 100% real, actionable, timely, and contextual insights into threats and threat actors. This empowers security teams to identify, prioritize, and effectively mitigate digital security risks. Leveraging attackers’ perspectives, KELA’s platform helps clients uncover hidden risks, fostering a proactive cyber defense.

P: +61 2 9338 2600
E: info@mcgrathnicol.com
W: www.mcgrathnicol.com



Slipstream/ Interactive

As a premier cyber security provider in Australia, Slipstream Cyber, a part of Interactive, offers end-to-end cyber security management from strategy and optimisation, through to incident response. Our services, including Active Defence, Consulting, Digital Forensics and Incident Response (DFIR), and Technical Assurance, are designed to fortify your defences and ensure uninterrupted business operations.

At Slipstream Cyber, we take pride in our 100% sovereign status and true 24x7 Managed Threat Detection, Incident Response, and Consulting capabilities. With offices strategically located in Perth, Sydney, and Melbourne, our fully staffed Cyber Security Operations Centre (SOC) operates around the clock, providing constant vigilance against cyber attacks.

We were the first Security Operations Centre in Australia to achieve CREST accreditation, underscoring our commitment to excellence and innovation. Our highly qualified and vetted team, coupled with ISO27001 certification and CREST and DISP accreditations, delivers specialist tools, techniques, and expertise to defend against all forms of cyber threats.

W: <https://www.slipstreamcyber.com/>



FTI Consulting

FTI Consulting is an independent global business advisory firm dedicated to helping organisations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals (located in all major business centres globally) work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities.

Our Cybersecurity practice is integrated into a broad range of related solutions, including global investigations, forensic accounting and technology, data and analytics, data privacy and protection, crisis management and strategic communications, and anti-money laundering. Our global team consists of hundreds of dedicated cybersecurity experts, incident response consultants, developers, and data scientists with extensive investigative backgrounds, led by those with decades of experience at the highest levels of law enforcement, prosecuting offices, intelligence agencies, and private sector institutions.

We build a safer future by helping organisations:

- Understand their own environments
- Harden their defences
- Rapidly & precisely hunt threats
- Holistically respond to crises
- Recover operations & reputation after an incident.

P: +61 2 8247 8000
W: www.fticonsulting.com/Australia





CrowdStrike

CrowdStrike, a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

CrowdStrike: We stop breaches.

W: <https://www.crowdstrike.com.au/>



Triskele Labs

We are one of Australia's fastest-growing cybersecurity companies. Our approach to exceeding expectations and delivering tailored services is truly one of a kind. We care, it's part of our culture, and you will notice the difference.

Our people are amongst the country's most certified and experienced advisory, offensive and defensive Cybersecurity experts. And when it's your data, systems and people on the line, experience does matter.

We believe in delivering robust outcomes and solutions that defend, protect and manage your networks and systems to mitigate risks.

P: 1300 24 Cyber
E: commercials@triskelelabs.com
W: <https://www.triskelelabs.com/>



Huntsman

Huntsman Security, an Australian software company, has been at the vanguard of automated cybersecurity risk assessment and reporting for more than 20 years. Huntsman delivers data-driven risk management, analysis and reporting technology to provide confidence and clarity to security, risk and executive teams in their security decision making.

P: +61 2 9419 3200
E: info@huntsmansecurity.com
W: <https://www.huntsmansecurity.com/>



Logicalis

We are Architects of Change™. At Logicalis, we harness our collective technology expertise to help our clients build a blueprint for success, so they can deliver sustainable outcomes that matter. Our lifecycle services across cloud, connectivity, collaboration and security are designed to help optimise operations, reduce risk and empower employees.

P: 1300 724 745
E: enquiries@au.logicalis.com
W: <https://www.au.logicalis.com/>



KordaMentha

KordaMentha is an independent advisory firm providing specialist cybersecurity, financial crime, forensic, performance improvement, real estate and restructuring services across Asia-Pacific. We are experts in cyber risk, incident response and organisational strategy, compliance and reporting.

P: +61 2 8257 3000
E: info@kordamentha.com
W: <https://kordamentha.com/home>



Norton Lifelock/ Gen Digital

Norton Cyber Risk Solutions can provide a strategic breach response plan that can include identity theft protection, 24/7 customer support, and more so you can confidently continue to do business. Gen brings award-winning products and services in cybersecurity, online privacy and identity protection to more than 500 million users in more than 150 countries.

LI: [linkedin.com/GenDigital](https://www.linkedin.com/company/gen-digital)
W: <https://www.gendigital.com/us/en/>





Arize Communications

Arize Communications is a specialist communications agency offering expert public relations, communications and reputation management services. In a world saturated with content, standing out for the right reasons has never been more challenging or essential.

A strategic communications plan is like an insurance policy for your reputation.

P: 03 9977 4852
E: crisis@arize.com.au
W: www.arize.com.au



Baker Tilly

Baker Tilly US, LLP (Baker Tilly) is a leading advisory CPA firm, providing clients with a genuine coast-to-coast and global advantage in major regions of the U.S. and in many of the world's leading financial centres. Baker Tilly has extensive experience in quantifying business interruption risk exposure and losses arising from both traditional risks, such as fire and mechanical breakdown, and emerging risks.

P: +61 2 8488 6000
W: www.bakertilly.com



Flashpoint

Flashpoint is the pioneering leader in threat data and intelligence. We empower commercial enterprises and government agencies to decisively confront complex security challenges, reduce risk, and improve operational resilience amid fast-evolving threats. Our solutions span cyber threat intelligence, vulnerability intelligence, geopolitical risk, physical security, fraud and brand protection.

P: 888-468-3598
E: sales@flashpoint.io
W: <https://flashpoint.io/>



Forensic IT

Forensic IT stands at the forefront of Digital Forensics and Cyber Incident Response (DFIR), dedicated to delivering top-tier service and expertise. We specialise in tailoring cost-effective solutions to meet the unique needs of each client, ensuring they receive the best possible support. Forensic IT provide unwavering support and expert service in Digital Forensics and Cyber Incident Response.

P: 1300 018 114
E: enquiries@forensicit.com.au
W: www.forensicit.com.au



Cythera

Cythera is an Australian cybersecurity company with in-house cybersecurity professionals providing world-class cyber protection to medium to large companies and businesses all over Australia from the Cythera offices across Australia. You are never just a ticket number with us; our network engineers know all our clients by name, and we protect your ICT networks as if it were our own.

P: 1300 CYTHERA (1300 298 437)
E: sales@cythera.com.au
W: www.cythera.com.au

Clyde & Co respectfully acknowledges the Traditional Custodians of the lands on which we live, work and gather. We acknowledge the Gadigal people of the Eora Nation where our head office is based, and the Traditional Custodians of the lands across this nation where our offices are located. We recognise their continuing connections to lands, waters and cultures. We pay our respects to Elders, both past and present. We also extend that respect to all our First Nations team members and clients.



480

Partners

2,400

Lawyers

5,000

Total staff

3,200

Legal professionals

60+

Offices worldwide*

www.clydeco.com

*includes associated offices

Further advice should be taken before relying on the contents of this summary.

Clyde & Co accepts no responsibility for loss occasioned to any person acting or refraining from acting as a result of material contained in this document. No part of this document may be reproduced without the prior permission of Clyde & Co. Clyde & Co Australia is a multi-disciplinary partnership registered with the Law Society of New South Wales.

© Clyde & Co LLP 2022

Key contacts



Reece Corbett-Wilkins

Partner, Sydney
+61 2 9210 4984
reece.corbettwilkins@clydeco.com



John Moran

Partner, Sydney
+61 2 9210 4974
john.moran@clydeco.com



Richard Berkahn

Partner, Sydney / Auckland
+61 2 9210 4981/ +64 9 801 0916
richard.berkahn@clydeco.com



Stefanie Luhrs

Partner, Brisbane
+61 7 3234 3038
stefanie.luhrs@clydeco.com



Alec Christie

Digital Risk Partner, Sydney
+61 2 9210 4510
alec.christie@clydeco.com



Andrew Brewer

Director, Cyber Risk, Brisbane
+61 7 3234 3005
andrew.brewer@clydeco.com



Chris McLaughlin

Cyber Risk Advisory Principal, Sydney
+61 2 9658 2880
chris.mclaughlin@clydeco.com



Richard Martin

Director Communications, Cyber, Sydney
+61 2 9658 2882
Richard.Martin@clydeco.com

We also want to acknowledge and thank the team for pulling this report together:

- Suzannah Hills
- Beccy Cambridge
- Laura Newton
- Jacky Li
- Stuart Lloyd
- Caitlin Bellis
- Aimee Johnstone
- Linda Tran
- Grace Donnelly
- Klara Vroljak
- Laurien Hush
- Michelle Nisbet