Clyde&Co
One

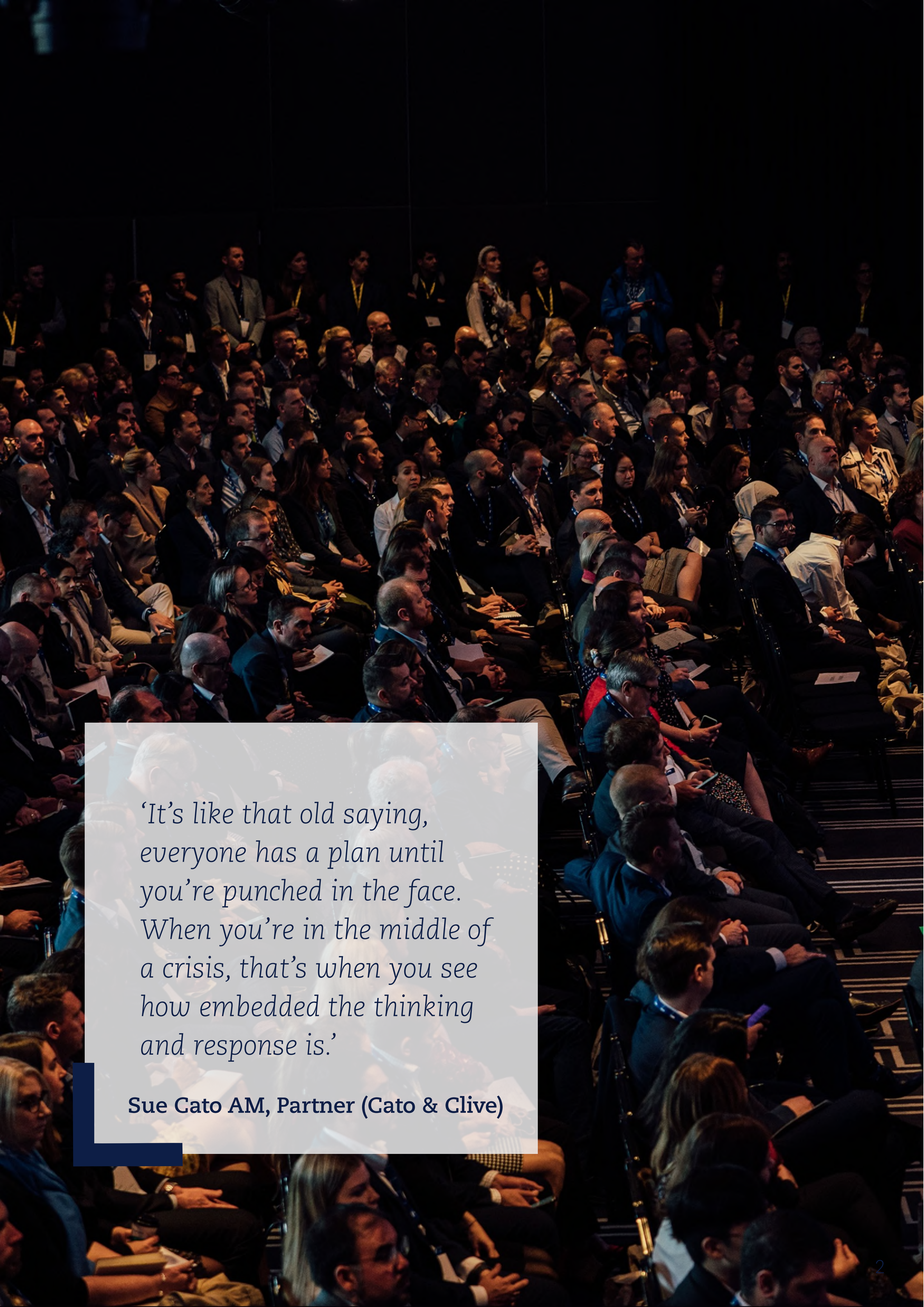
18 May 2023

Insights from the Cyber Summit

Readiness

Response

Recovery



> *'It's like that old saying, everyone has a plan until you're punched in the face. When you're in the middle of a crisis, that's when you see how embedded the thinking and response is.'*

Sue Cato AM, Partner (Cato & Clive)

#ClydeOneSummit
Readine
DOLTONE HOUSE

Contents

Foreword: reflections on the Summit

On 18 May 2023, Clyde & Co's Cyber, Digital Law and Disputes team hosted its inaugural Cyber Summit bringing together over 650 industry professionals, including government, insurers, brokers, company directors, lawyers, risk professionals, IT professionals, and technical specialists.

With a focus on 'Readiness, Response, and Recovery', the Summit explored various topics that will contribute to shaping and supporting the national objective for Australia to become the world's most cyber secure nation by 2030.

A 'first of its kind' for a law firm, the Summit hosted a tremendous line-up of over 30 speakers from Government, private practice, and clients, who shared their first-hand strategic insights and practical experience across a wide range of topics.

The feedback was overwhelmingly positive and presented a rare opportunity for leaders in Government, insurance, and private industry to join forces and share insights into the cybersecurity, legal, policy and risk landscape.

We are delighted to announce that the Summit will continue in 2024, and will be bigger and better than before.

We hope to see you there!

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

Watch the opening remarks here.

Session overview

1

Clyde & Co's **John Moran**, NSW Privacy Commissioner, **Samantha Gavel**, **Matt Smith** (Assistant Director General Incident Management Branch, ACSC/ASD), **Detective Superintendent Matt Craft** (NSW Police), and **First Assistant Secretary Brendan Dowling** (Department of Home Affairs) kicked off, discussing the upcoming legislative reforms introducing a Mandatory Notifiable Data Breaches Scheme in NSW, the ACSC's 12-18 month agenda and the impact this will have on how entities manage incident response, and key priorities for law enforcement to tackle cybercrime (see page 8).

2

Robyn Ziino (Group Chief Privacy Officer and Global Data Retention Officer, Westpac), **Darren Kane** (Chief Security Officer, NBN Co), and **Chris Burubu** (General Counsel and Company Secretary, Business NSW) joined Clyde & Co's **Chris McLaughlin** and **Alec Christie** to discuss industry-leading data collection and retention practices (see page 10).

3

Clyde & Co's **Reece Corbett-Wilkins**, **James Blakely** (Director), and **Jacqueline Wilson** (Lead – Stakeholder Engagement and Community Education) outlined the role of ID Support NSW and how their team assists entities to manage their post-breach consequence management response to support impacted individuals. More details of this session can be found at page 12.

4

Clyde & Co's **Richard Berkahn** was joined by **Jacquie Shanahan** (General Counsel and Company Secretary of Isentia Group), **Rhian Greenway** (Chief Information Officer at City Beach), and **Timothy Rabbitt** (Managing Director & CEO of Acumentis) to discuss their first-hand experiences navigating an entity through a cyber incident.

This session provided attendees with a rare insight into how other entities manage a board through the crisis-management process, and their experiences liaising with key stakeholders including regulators and the market (see page 14).

5

Looking forward, **Gavin Beardsell**, Senior Investment Manager and Legal Counsel at prominent litigation funder, Omni Bridgeway, and **Martin del Gallego**, an experienced class action Partner at Piper Alderman joined Clyde & Co's **John Moran** to explore the future cyber claims landscape.

The panel particularly focussed on the recent increase in class actions following the Medibank and Optus breaches, and provided insight into how non-economic loss will be considered by Courts in the future (see page 17).

6

Attendees then heard a keynote address from Insurance Council of Australia CEO and Managing Director, **Andrew Hall**, outlining the role the insurance industry will play in achieving Australia's cyber security vision, and how regulatory harmonisation can bring about that outcome (see page 21).

7

We also considered how Australia's privacy regulatory landscape differs from overseas counterparts in New Zealand and the UK in a discussion with Clyde & Co UK's Ian Birdsey, and Clyde & Co's Australia and New Zealand's Richard Berkahn and Anthony Cooke.

The session outlined what Australia can learn from other jurisdictions, and provided insight into what changes might be implemented to reflect regulatory schemes internationally (see page 24).

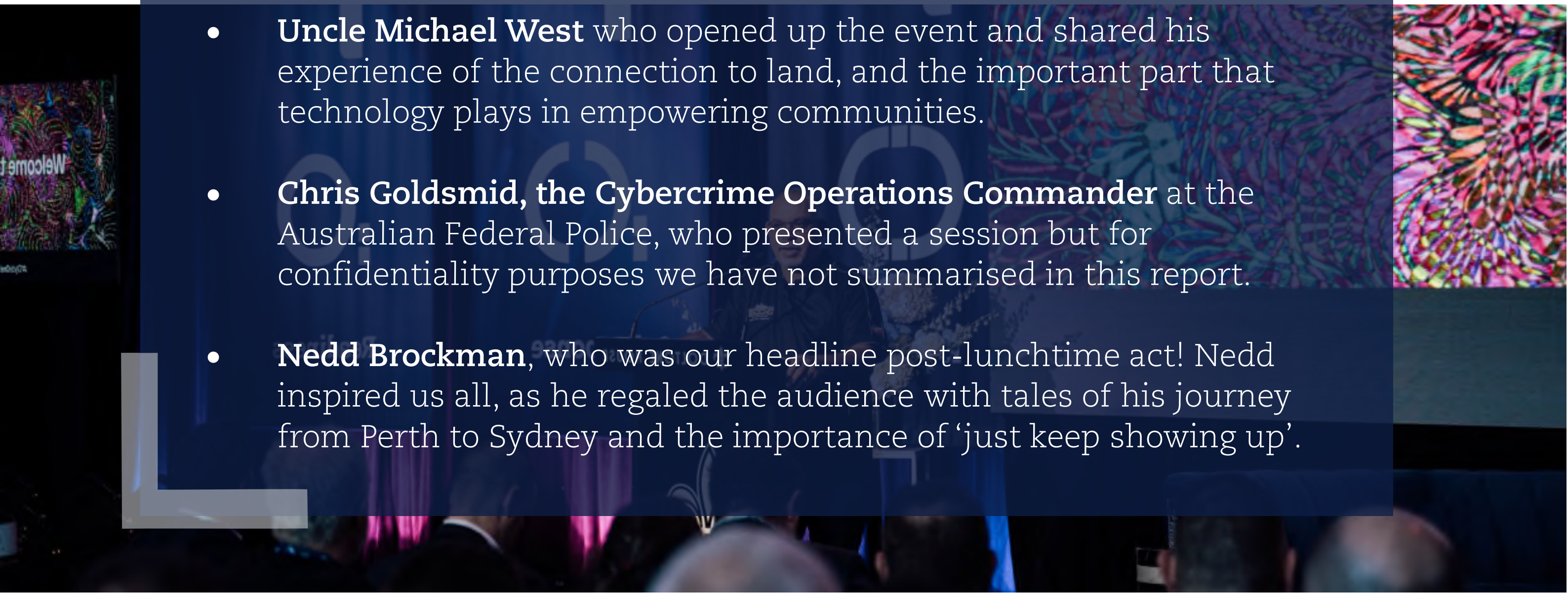
8

To conclude the Summit, Clyde & Co's Reece Corbett-Wilkins spoke with corporate communications advisor Sue Cato AM (Partner at Cato & Clive) and public affairs advisor Jody Fassina (Managing Director of Insight Strategy) about what effective communication looks like in a cyber crisis, and how to manage a diverse stakeholder base (see page 26).

Acknowledgements

We also wish to acknowledge and thank the following people:

- **Uncle Michael West** who opened up the event and shared his experience of the connection to land, and the important part that technology plays in empowering communities.
- **Chris Goldsmid, the Cybercrime Operations Commander** at the Australian Federal Police, who presented a session but for confidentiality purposes we have not summarised in this report.
- **Nedd Brockman**, who was our headline post-lunchtime act! Nedd inspired us all, as he regaled the audience with tales of his journey from Perth to Sydney and the importance of 'just keep showing up'.



Cyber transformed

Regulation, privacy, law enforcement and incident response

While the Optus and Medibank incidents in 2022 can be considered 'worst-case scenarios', they also represented a major turning point towards the realisation that further action is required to ensure Australia is better protected from cyber incidents in the future.

The call is for governments, industries, organisations, and individuals to come together to contribute to a coordinated effort in boosting cyber readiness, response, and recovery.

This session outlined the role of law enforcement in assisting entities to respond to a cyber incident, what entities can do to improve their cyber resilience, and how we can all contribute to improving Australia's cyber security.

As recently stated by Australia's Cyber Security Minister, Clare O'Neil, on a recent interview with the Risky Business podcast – 'data breaches aren't just private events that just affect private companies. They are of public interest and are a national security incident'.

Consider the type of data you are holding and the risks involved.

Commissioner Gavel emphasised the importance of entities going 'back to privacy basics' and ensuring that they are only collecting and retaining the data they need.

Commissioner Gavel also emphasised the importance of entities understanding where their data is kept, and importantly whether it needs to be retained. Once it is determined that certain data is no longer needed, then organisations must ensure that they dispose of it securely.

To effectively recover from a cyber incident, it is important to prepare in advance

Matthew Craft outlined that many businesses are unprepared for cyberattacks as they have not considered business continuity plans.

The top priority for a business suffering from a cyber incident is to get systems back online, rather than gathering evidence for a later investigation.

Brendan Dowling also highlighted that paying a ransom does not necessarily get a business out of a tough situation. Just because a business gets it's data back, doesn't mean the data has not been exfiltrated. Accordingly, there remains a residual risk of data misuse.

Matthew Craft emphasised the importance of organisations having an incident response plan, including a ransomware 'playbook', in place and ensuring that it is tested. This offers a structured framework that guides a response rather than waiting for an incident to occur. He also recommended ensuring that incident response plans are retained in hard copy to ensure accessibility in circumstances where an entity's system is offline.

Understand what resources and support you have available to respond to cyber incidents

Matthew Smith emphasised that there is support available to all organisations and a key step is reporting an incident to the ACSC which allows an entity to receive immediate advice regarding how to manage the incident.

The ACSC's focus is on how to help the next victim. It achieves this through gathering intel regarding specific threat actors involved in reported incidents, and consolidating this intelligence into a knowledge database so that it can be leveraged to assist the next victim.

A remaining challenge is ensuring Australia has enough resources to respond to cyber incidents. Not all organisations that are attacked will have the same resources as large businesses such as Optus and Medibank.

What can entities do now:

1. Consider the consequences that can arise from the type of data you are holding having regard to how sensitive it is and look to update your policies to ensure compliance with relevant regulations, improve data security, and implement policies to facilitate efficient data management.
2. Assess the effectiveness of your current response capabilities and incident response plans and identify any areas for improvement. This should include board and management roles and responsibilities, arrangements with incident response service providers, legal and regulatory obligations, as well as training to educate your people on what to do in such circumstances.
3. Ensure you have a sound business continuity management system in place and assess it against the requirements outlined in the ISO 22301 standard to identify gaps and strengthen your business continuity management practices.

The Art of Letting Go

Data discovery and destruction

While the digital economy promotes the idea that 'data is the new oil' and therefore of value, data can be both an asset and a compliance liability to an organisation.

There is a strategic balance to be struck to maintain the operational strength of the organisation and its innovative demands and use for its data, as well as mitigating the risks of holding such data and complying with its legal obligations.

With the prevalence of data accumulation by organisations, the recent publicised large data breaches in Australia, and the increase in penalties for non-compliance, managing the risks of data holdings should be a high priority for all organisations.

The secrets to a successful data retention and destruction program

Engagement:

Engaging with everyone in your organisation means you can:

- gain a deeper understanding of the data that is being collected and retained,
- address the operational needs of the business, and
- ensure the data management measures can effectively meet the risks and compliance obligations.

Education:

There should be strong awareness of data governance through the organisation, with the risks of collecting and retaining data being '*top of the mind*' of management and all teams (beyond the cyber and information security group). This will ensure all stakeholders own this business risk and are invested in the data retention and destruction plan.

Education is also a corrective reminder when business teams speak of '*our data*' as it is an individual's data that they have been entrusted with to secure and protect it from interference, misuse and unauthorised access and to '*do the right thing to maintain it*'.

De-identification of data is an effective tool when there is no option to delete the data

The Attorney-General's Privacy Act Review proposes to apply certain obligations under the Privacy Act to de-identified data where there is no option for deletion or there is a need for aggregated use of the data.

However, de-identification is an inadequate substitute to deleting data and any technology used for de-identification must be continually reassessed to determine if the data remains de-identified over time.

Practical tips to implementing data retention and destruction programs:

The panel emphasised that for many organisations, it is important to know **what** data the organisation holds, **why** it holds such data and understand the risks of inadequate data retention and destruction strategies (or **when**) you should get rid of it.

Here are some actions you can take now towards better data governance:

1. **Establish a good process** - adapt systems and adopt a culture across the organisation to achieve better data management and resilience. It is not done and dusted when a policy is in place, it's an ongoing journey.
2. **Adjust the program's approach to the risks** - engage external advice and support to determine the best and most efficient approach. Take the data governance journey one step at a time.
3. **Know your suppliers and what they are doing with the data** - manage your third-party risk too.
4. **Do not leave data management up to too few in the organisation** - ensure everyone understands good data governance and risk management.
5. **Invest in communications** - so the data management message is understood and the approach to data retention and destruction is consistent and effective.

> *'…for those that have business ownership of data – you own the risk. That is, it's your risk to make sure the data has value, you own the risk to make sure where that data is located, and the risk to know who has access to the data, most importantly you own the risk to how it's protected and who's protecting it.'*
>
> **Darren Kane, Chief Security Officer, NBN Co**

ID Support NSW Keynote

Identity theft, remediation support, community education

After several breach events suffered by Government Agencies, one being the Service NSW breach in 2020, it became obvious that 6 months to notify customers of a breach wasn't good enough when it takes roughly 20 days from theft to misuse of data.

The NSW Government has now released the NSW Government Identity Strategy and new laws were created to allow Government Agencies to talk to each other. This included establishing ID Support NSW to be a one stop shop for businesses and individuals impacted by identity theft and data breaches and to assist NSW customers, NSW businesses and NSW Government Agencies.

Timely and accurate analysis significantly changes the landscape for individuals affected.

The team at ID Support NSW can offer critical and objective analysis of personal information risk to entities who have suffered a breach incident to help clarify messaging about remediation.

This came in the wake of research which revealed that without clear messaging some individuals were spending around 34 non-consecutive hours to remediate and recover their identity following a breach.

ID Support NSW assist with clarifying an entity's post-breach and remediation messaging issued to impacted individuals, to ensure that an entity is not wasting time and money on costly remediation to assist individuals to recover their identity, if it is not necessary.

For example, the Optus breach affected the personal drivers licence numbers of 1.2 million people. Following critical and objective analysis of the personal information impacted, and a review of datapoints of the licences affected, it was possible to narrow that number down to 17,000 licences that needed to be remediated.

Streamlining government agencies to form a collective approach can impact the timeline and remediation abilities

By utilising existing teams within Government to conduct audits on the process of remediating identity documents, it was possible to identify pain points including inconsistent communication across agencies and departments.

Enabling Government agencies to talk to each other has reduced the necessity for individuals and business to interact with multiple agencies. Further, refining the process and reducing the need to complete multiple steps and forms, has meant victims spend less time repeating the same processes.

This not only gives customers back precious hours, but also encourages victims to complete the process and to remove the compromised documents from circulation.

Setting up the National Coordination Mechanism (NCM) and the National Emergency Management Agency (NEMA) to provide a cohesive whole of government response

If you have suffered a data breach involving multiple ID types, then you will ordinarily be required to speak to individual Government agencies in each state to reissue.

The National Coordination Mechanism (**NCM**) was established in COVID-19 to assist with disaster management. One of the sub-plans of this covers cyber security. The NCM is coordinated through the National Emergency Management Agency, to provide a more streamlined mechanism for an entity to respond to an emergency.

ID Support NSW will represent the NSW issuing agencies, reducing the need for multiple conversations within government across NSW, which naturally reduces the timeline to respond.

What will this look like 10 years from now?

Digital Identity is not a silver bullet, but it would go a long way to removing the usual identification documents from circulation. Instead of using you drivers' licence, Medicare card, and birth certificate you could use your Digital Identity. This puts the power back in the hands of each individual and allows them to choose when and what credentials are used to validate their identity.

> *'If a NSW driver's licence was exposed in a data breach and we were able to render that useless in a matter of minutes by blocking it essentially, I feel like that would pull those licences out of circulation and a driver's licence wouldn't be such a valuable thing to steal.'*
>
> **Jacqueline Wilson, Lead Stakeholder Engagement and Community Education, ID Support, NSW Dept of Customer Service**

Stories from the frontline

Client panel sharing real world cyber incident experiences

In an increasingly interconnected digital world, the rise of large-scale cyber-attacks has become a grim reality that businesses can no longer afford to ignore. Often, these cyber-attacks can leave unprepared organisations vulnerable to devastating consequences which can threaten the survival of their organisation.

To shed light on the gravity of this issue, Clyde & Co were joined by panelists who had themselves navigated a cyber incident, to explore how some organisations have overcome the daunting struggle of not knowing where to begin when they've first been hit, and how they ultimately coped with tackling a significant cyber breach.

Dealing with different types of cyber incidents – a view from the top

Ranging from business email compromises, ransomware attacks to an insider threat, our panelists shared firsthand accounts of what it was like to deal with these incidents in their respective roles.

Timothy Rabbitt - CEO and Managing Director at Acumentis

Timothy Rabbitt shared his experience with an insider threat, which can be particularly difficult to deal with – compared to the ransomware attacks that are more often receiving media attention.

Timothy Rabbitt highlighted how often the toll on staff caused by a cyber event, and in particular the impact to morale, is often overlooked by entities and can linger for a significant period post-incident.

> *'Cyber security is not just an IT function in your team…it's a whole team effort.'*
>
> **Timothy Rabbitt, CEO and Managing Director, Acumentis**

In the end, clear communication and managing their board effectively to execute action items helped limit the impact on staff morale in a time of uncertainty.

In this respect, Timothy Rabbitt emphasised the importance of engaging with regulators early and often. Rabbitt also highlighted that a good board makes a big difference to being able to act swiftly when dealing with cyber-attacks and that incidents can have a silver lining in that they can bring a business closer together.

Rhian Greenway - CTO at City Beach

Rhian Greenway offered insights on how his organisation dealt with a cyberattack which occurred in the early hours of the morning prior to a long week and spun into full force quickly. This experience demonstrated how important it is for a business to be able to quickly engage a full business crisis response which simultaneously prioritises business continuity with containment and remediation.

Rhian Greenway outlined how the business was able to quickly engage its IT and legal teams and how 'pulling the plug' early had assisted in preserving key business assets. Rhian Greenway's key piece of advice was how important it was for businesses to forgo the 'it won't happen to us' approach and implement a right-sized approach for the purposes of effective resource allocation.

Rhian Greenway emphasised how in the aftermath of an incident, the business' approach to cyber investment spend and data retention changed for the better, and recommended that businesses go to market regularly to ensure they have cutting edge technology rather than relying blindly on pre-existing ICT relationships.

Jacquie Shanahan - General Counsel at Isentia

Jacquie Shanahan provided insight to some of the notable difficulties for boards managing a cyber incident namely: keeping informed, navigating uncertainty, managing the Board's role, and knowing what steps to take and when.

Jacquie Shanahan emphasised the importance of good cyber communications strategy in a crisis to effectively manage key stakeholders. She also recommended that businesses undertake scenario planning exercises and ensure they develop a suite of advisors pre-incident to ensure that they know who to turn to in a crisis.

What you can do now

The alarming truth is that many businesses remain drastically underprepared to handle a severe cyber breach. Here are some practical things you can do now to ensure you are better equipped.

1. **Have a full business response ready to hit the ground running**. In particular, an action plan to get the business back online and operating as soon as possible is crucial.

2. **Invest in the right things and invest in education of your people.** Ensure you have real-time response tools that you can rely on in the event of a cyber breach. For example, go to the market every 12 months to ensure you have the most up-to-date ICT infrastructure.

3. **Be prepared to manage expectations in the event of a cyber-attack**. By addressing the challenges and potential setbacks, you can build trust within the organisation and mitigate the psychological toll of a cyber breach. Managing expectations allows more effective allocation of limited resources, for example when a business understands its own needs, it can prioritise response efforts in that area.

The claims horizon

Incident remediation, duties of directors, and class actions

While there are many factors at play which support the growing prevalence of privacy-related class actions in Australia, there are also a number of obstacles for individuals to navigate in order to bring a successful claim. Our expert panel agrees that the litigation risk stemming from data breaches is something that should be front of mind for organisations.

Our panel discusses the current data breach class action landscape in Australia, including recent developments and international trends likely to influence the frequency of these types of claims.

What are the challenges facing claimants?

While there has been an explosion of privacy-related class action activity overseas, there are a number of challenges for Australian claimants to bringing – and ultimately succeeding in – a data breach class action. Notably, the absence of a clear cause of action and difficulties around proving and quantifying loss suffered as a result of a data breach.

No clear cause of action for claimants

Despite heightened judicial discourse in recent years, Australian courts are yet to confirm the existence of a common law tort of breach of privacy. This stands in contrast with developments in similar jurisdictions, such as New Zealand, the United Kingdom and the United States, all of which recognise a more general right of privacy.

Instead, impacted individuals may:

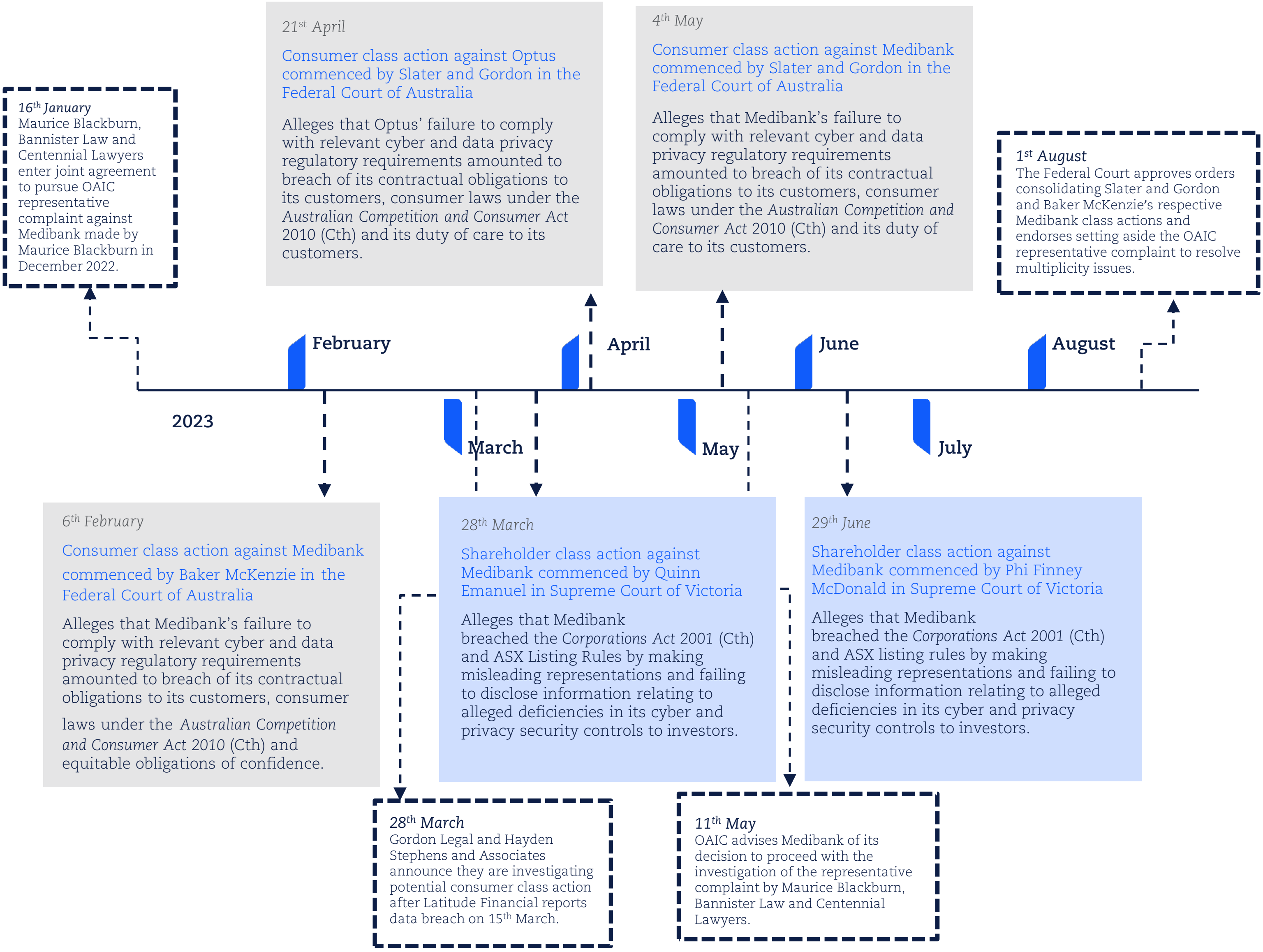
- make a representative complaint for breach of the *Privacy Act 1988* (Cth) to the Office of the Australian Information Commissioner; or
- bring a claim under a range of other causes of action, based on the nature of the claim and their relationship with the impacted organisation.

Taking the audience through *Evans v Health Administration*[1] (Australia's first data breach class action) and recent privacy-related claims brought against leading Australian private health fund, Medibank Private, del Gallego highlights the key causes of action that claimants are relying on:

- breach of contract (the impacted organisation's conduct leading to the breach was a breach of a contractual agreement with the claimants);
- breach of confidence in equity (the impacted organisation mismanaged the claimants' personal information entrusted to it in confidence);
- negligence (the impacted organisation failed in its duty of care to protect claimants' data from misuse which resulted in harm); and

[1] [2019] NSWSC 1781.

Image (below): Key events in the Australian data breach class action space in 2023 so far



16th January
Maurice Blackburn, Bannister Law and Centennial Lawyers enter joint agreement to pursue OAIC representative complaint against Medibank made by Maurice Blackburn in December 2022.

6th February
Consumer class action against Medibank commenced by Baker McKenzie in the Federal Court of Australia

Alleges that Medibank's failure to comply with relevant cyber and data privacy regulatory requirements amounted to breach of its contractual obligations to its customers, consumer laws under the *Australian Competition and Consumer Act 2010* (Cth) and equitable obligations of confidence.

28th March
Shareholder class action against Medibank commenced by Quinn Emanuel in Supreme Court of Victoria

Alleges that Medibank breached the *Corporations Act 2001* (Cth) and ASX Listing Rules by making misleading representations and failing to disclose information relating to alleged deficiencies in its cyber and privacy security controls to investors.

28th March
Gordon Legal and Hayden Stephens and Associates announce they are investigating potential consumer class action after Latitude Financial reports data breach on 15th March.

21st April
Consumer class action against Optus commenced by Slater and Gordon in the Federal Court of Australia

Alleges that Optus' failure to comply with relevant cyber and data privacy regulatory requirements amounted to breach of its contractual obligations to its customers, consumer laws under the *Australian Competition and Consumer Act 2010* (Cth) and its duty of care to its customers.

4th May
Consumer class action against Medibank commenced by Slater and Gordon in the Federal Court of Australia

Alleges that Medibank's failure to comply with relevant cyber and data privacy regulatory requirements amounted to breach of its contractual obligations to its customers, consumer laws under the *Australian Competition and Consumer Act 2010* (Cth) and its duty of care to its customers.

11th May
OAIC advises Medibank of its decision to proceed with the investigation of the representative complaint by Maurice Blackburn, Bannister Law and Centennial Lawyers.

29th June
Shareholder class action against Medibank commenced by Phi Finney McDonald in Supreme Court of Victoria

Alleges that Medibank breached the *Corporations Act 2001* (Cth) and ASX listing rules by making misleading representations and failing to disclose information relating to alleged deficiencies in its cyber and privacy security controls to investors.

1st August
The Federal Court approves orders consolidating Slater and Gordon and Baker McKenzie's respective Medibank class actions and endorses setting aside the OAIC representative complaint to resolve multiplicity issues.

- breach of general statutory obligations (e.g., the impacted organisation engaged in misleading or deceptive conduct or breached continuous disclosure obligations).

Quantification of loss in data breach class actions

Even if the requirements of a particular cause of action are met, claimants will need to prove and quantify the loss suffered as a result of the breach.

Drawing on his experience managing a number of Australia's largest and most high-profile cyber incidents to date, John notes that it can be challenging to put a monetary value on the harm caused as a result of a breach – impossible in some cases.

Quantification of loss may be relatively easy when a data breach leads to direct financial loss or a measurable decline in share value. In circumstances where an individual's sensitive personal information has been compromised, however, it can be difficult to measure loss such as the harm caused by damage to reputation or emotional distress.

Until the first round of class actions makes their way through Australian courts, the question remains open as to how lawyers and claimants will approach quantifying the non-economic loss flowing from data breaches.

What does the path ahead look like?

Despite these hurdles, Martin believes that plaintiff law firms in Australia are getting braver and have clearly expressed an appetite to take on the challenge of data breach class actions.

While claims based on largely untested causes of action would not typically attract funding, litigation financiers are also more willing to deploy capital into these types of actions.

Speaking about the assessment process for funding applications, Beardsell noted that data breach class actions are not differentiated from other types of class actions. Instead, the focus is on the prospects of a meaningful recovery, for all parties, based on the merits and quantum of the claim.

Cyber-related class actions were the fourth largest category of class actions in the United States in 2022, totalling approximately USD 720 million in settlements[2] – a trend not gone unnoticed by Australian litigation financiers. As the frequency and severity of cyber-attacks in Australia continues to rise, the potential sum of individual losses is significant and increasingly attractive to funders.

[2] Source: Edward Segal, 2023, Class Action Lawsuits Set New Billion Dollar Settlement Records In 2022: Report, Forbes, <https://www.forbes.com/sites/edwardsegal/2023/01/04/class-action-lawsuits-set-new-billion-dollar-settlement-records-in-2022-report/?sh=1242654c2ef6/>

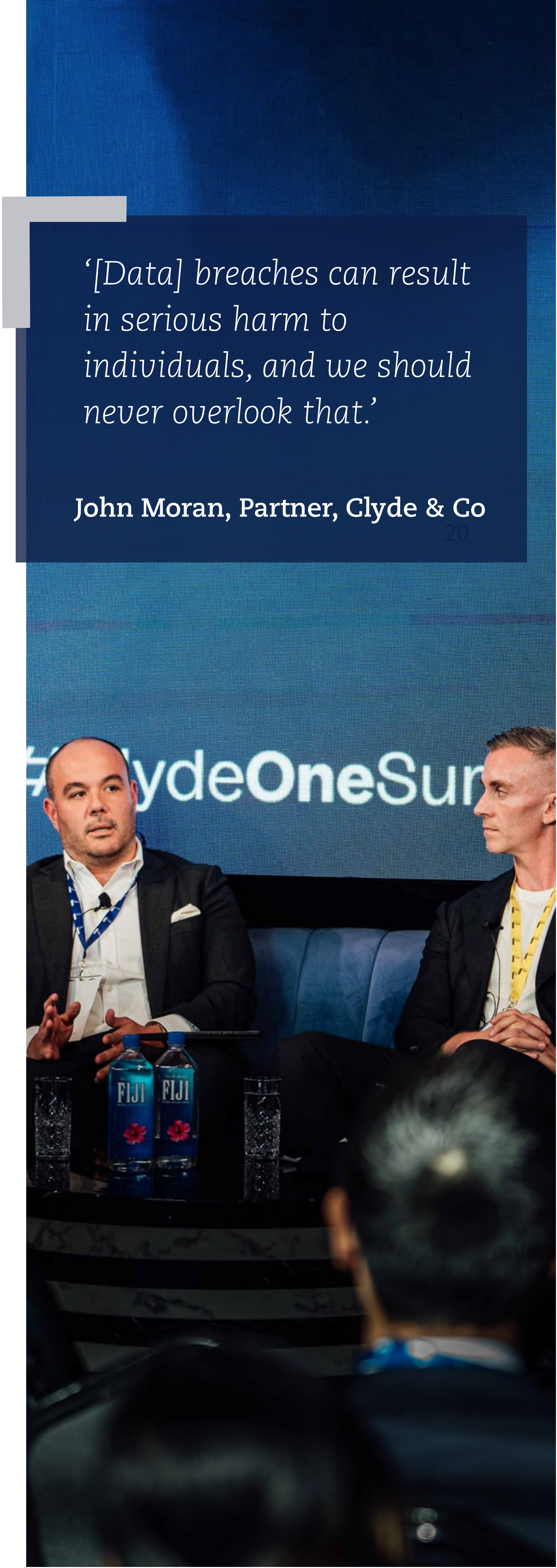
What does this mean for organisations?

These emerging claims risks are a complex new addition for Australian organisations who now have to contend with not only the significant costs of responding to a breach and possible regulatory action, but also the potential costs associated with high-risk class action litigation.

In closing, John recommends that organisations consider an incident response plan and insurance solution that factors in, not only getting 'back to business' and stakeholder communications, but also third-party remediation and the potential litigation risk.

Key takeaways

1. With large-scale cyber incidents on the rise, it is likely that more data breach class actions will be filed in Australian courts, following international claims trends.
2. Data breach class actions are normally founded on a broad range of causes of action that remain largely untested. Once the first wave of data breach class actions makes its way through Australian courts, claimants may have a clearer idea of whether such actions will give rise to meaningful results.
3. Organisations should nevertheless be mindful of the potential increase in activity in the data breach claims space and consider taking proactive measures to improve their cyber risk resilience in accordance with best practice.



> *'[Data] breaches can result in serious harm to individuals, and we should never overlook that.'*
>
> **John Moran, Partner, Clyde & Co**

Insurance Council of Australia Keynote

Australian Cyber Security Strategy, the role of insurance, adoption of a standalone Cyber Security Act, reporting and payment of ransoms

With an estimated 90% of cyber remaining uninsured, it is clear there is more work needed to protect business assets. A whole of nation approach is required between the Government and the business community to build greater resilience to cyber threats.

Andrew Hall, CEO of the Insurance Council of Australia, provided key insights on the insurance industry's perspective on how to tackle some of these challenges.

Cyber insurance in Australia

The increasing prevalence of cyberattacks has made the protection of digital assets as important as that of a business' physical assets. While the focus on cyber risks and cyber insurance is increasing, the role of cyber insurance is still not broadly understood, and the uptake is low compared to other insurance classes.

Government and the business community must work together to ensure that everyone understands the risks to build greater resilience to cyber threats.

Limitations

A significant problem lies in the small number of insurance providers offering cyber policies. The combination of a small premium pool, and the increasing sophistication and prevalence of cyber-attacks, has placed significant pressure on insurers and businesses alike.

Greater information sharing between Government and industry removes, at least in part, some of the roadblocks to the pricing of cyber risk. The business community should be providing as much intelligence to the Government as possible. In turn, the Government must de-identify and aggregate that information into digestible and actionable intelligence reports for industry.

Systemic risk remains a key concern. There is more work to be done between Government and industry to find a solution to the risks associated with catastrophic cyberattacks.

Regulatory harmonisation

The immediate priority for the Government must be on cleaning up the existing regulatory framework around cyber security. This includes the harmonisation of the existing 'patchwork of policies, laws, and frameworks'. Some of the immediate steps that should be taken include:

- providing further clarity on existing definitions in the Security of Critical Infrastructure Act;
- removing or streamlining duplicate obligations; and
- creating a single reporting portal for cyber incidents.

Fundamentally, improving the nation's cyber readiness cannot wait for the Government to introduce a new cybersecurity act.

National cyber posture

Hall continued to build on the theme of business and the Government working together, stressing that this collaboration needs to ensure that the small business community is not left behind. Hall noted that the country's defences are only as strong as their weakest link and urged the Government to partner with industry to demystify cybersecurity for the small business community.

Ransom payments

Many are still grappling with the difficult issue of ransom payments. The ugly truth is this, paying a ransom becomes necessary when a business' survival is at risk due to the lack of access to digital assets in a digital economy.

There is still adivide around the Government's proposal to ban ransom payments, with many arguing it would limit the ability of some firms to recover from cyber-attacks and drive reporting and payments underground. Some suggest there are other policy levers that the Government could deploy to ward off cyber criminals – including increased penalties and crypto-asset regulation.

Key takeaways

1. Business leaders across the country should understand cyber risk and prepare for an attack.

2. When businesses do fall victim to cyber-attacks, it is important that the Government is able to provide the necessary assistance as seamlessly as possible.

3. Those with insurance will have the added comfort and support needed to recover quickly. Ideally that should be 80% of a market, not just 20%.

4. While the challenges in the cyber space are big and growing, they are not without their solutions. The solutions can only be achieved by a unified, national projects involving all of Government, individuals, and businesses.

‘It is important that the business community is providing as much intelligence to Government as early and often as possible. In return, the Government must de-identify and aggregate into digestible and actionable intelligence reports for industry…this information sharing will help build a national trust-based ecosystem that will serve to improve Australia’s national cyber posture.’

Andrew Hall, CEO, Insurance Council of Australia

Crossing Borders

Evolving data protection laws, global regulatory developments, third-party litigation, fines and penalties

Cyber risk has captured the attention of the Government and the public like never before. Relative to many other countries around the world, Australia is well progressed in its privacy journey. That said, there is certainly a lot we can learn from other jurisdictions when it comes to privacy and data security.

In this session, we took a look across the UK, Australia and New Zealand at the current cyber risk landscape, some key challenges, and navigating the regulations across each jurisdiction.

UK and EU

On the other side of the globe, the GDPR governs data protection across the UK and most of Europe, and is arguably the most recognised piece of privacy legislation in the world. It imposes:

- burdensome compliance requirements for organisations;
- a broad definition of what constitutes personal information;
- significant extraterritorial scope; and
- low thresholds for reporting from a data breaches perspective.

Because of this, it has paved the way for governments worldwide to implement tougher and more comprehensive data protection regimes.

Regulators across the UK and EU have approached enforcement of the GDPR with vastly different expectations and agendas, largely as a reflection of each country's unique technological and political climate. This is also reflected in how fines and penalties have historically been handed down following breaches of the GDPR.

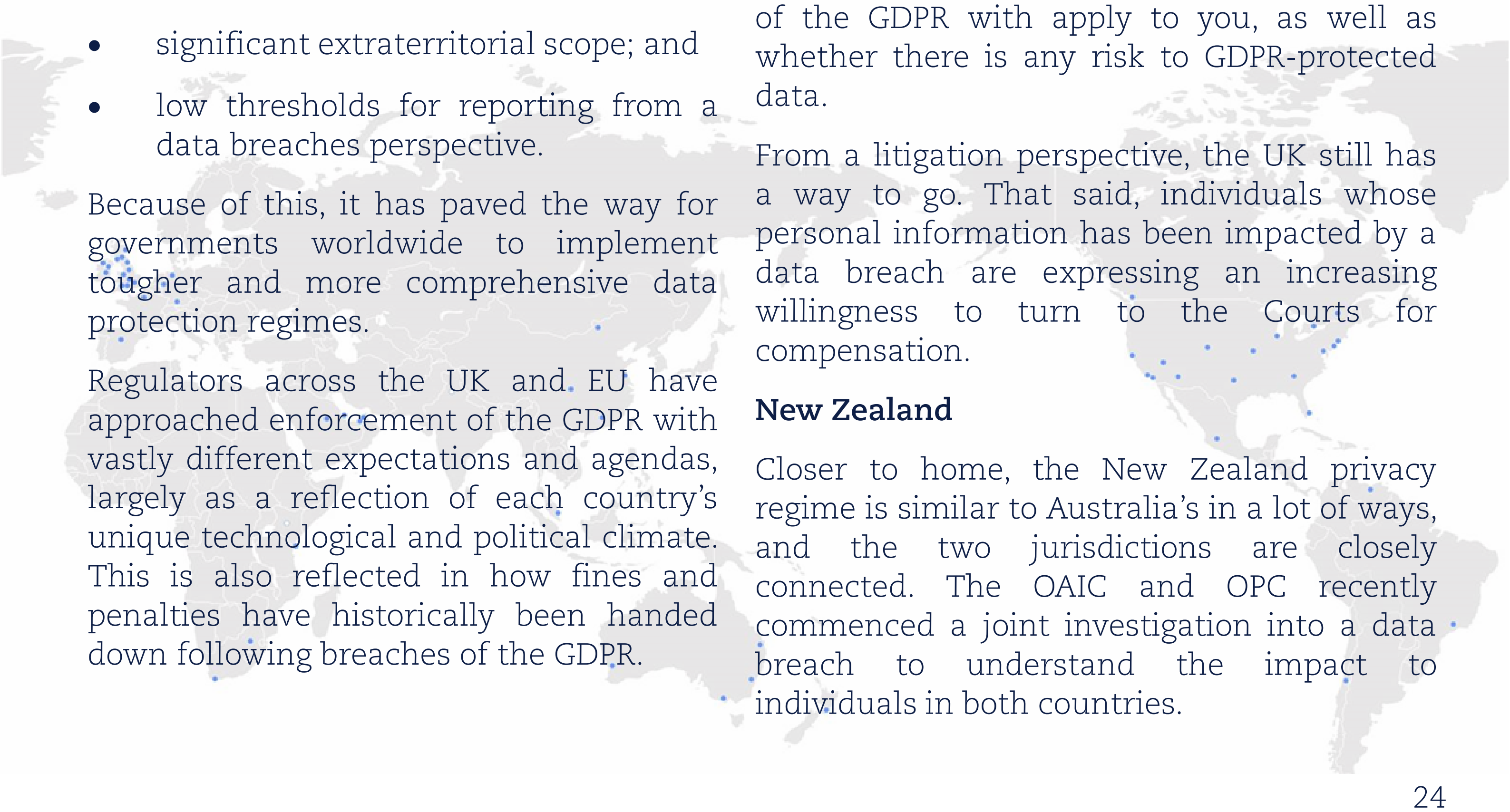
In managing a multi-jurisdictional data breach, it is difficult not to take a 'one size fits all' approach, and rather consider specific requirements for notification statements in each jurisdiction, and how each regulator is likely to respond.

Importantly for overseas organisations, the 72-hour clock does not necessarily start ticking as soon as you become aware you have experienced an incident – you must first understand whether the extraterritorial scope of the GDPR with apply to you, as well as whether there is any risk to GDPR-protected data.

From a litigation perspective, the UK still has a way to go. That said, individuals whose personal information has been impacted by a data breach are expressing an increasing willingness to turn to the Courts for compensation.

New Zealand

Closer to home, the New Zealand privacy regime is similar to Australia's in a lot of ways, and the two jurisdictions are closely connected. The OAIC and OPC recently commenced a joint investigation into a data breach to understand the impact to individuals in both countries.



That said, the New Zealand regime is closely modelled off the GDPR, and in many ways represents more of a middle ground approach between the GDPR and Australian privacy regime.

Similar to the GDPR, the New Zealand privacy regulator has issued guidance that notification of data breaches is expected within 72 hours after awareness (although this is not formally spelled out by the legislation). Early notification can stop the timer on regulatory scrutiny, and act as a powerful message to communicate to third parties that an organisation is proactively engaging with its responsibilities following an incident.

In comparison to the Australian OAIC, the OPC is an active regulator. Organisations that report immediately, and then regularly update the commissioner as the incident progresses, receive less scrutiny than organisations that delay. If the OPC considers that organisations are not being sufficiently proactive, it will encourage engagement through direct communication with general counsels or even with the media if necessary.

Australia

In Australia, there is some discussion around shortening the timeframe for notification. Unlike the regulators in the UK and New Zealand, the OAIC has expressly spoken out against early, precautionary notifications before a comprehensive assessment has been conducted. If Australia ultimately does shorten the notification timeframe, we can look to how organisations in the UK/EU and New Zealand have successfully managed compliance.

Over the past five years, the OAIC has played a passive game and been slow to actively engage with organisations following notification of a data breach. Following a string of high-profile incidents, increased attention, a boost in funding, and changing legislation, we have observed this position shift.

When it comes to privacy litigation, Australia has some precedent in the context of compensation for anxiety, stress, and trepidation, arising from a data breach. The idea of privacy-related class actions, and claims more broadly, is only just starting to bubble at the surface in Australia – which is in turn keeping a sharp eye on the UK litigation landscape.

Keeping eyes on the horizon

Despite the diversity of international regimes when it comes to incident response, there are common threads and learnings we can all benefit from when it comes to incident response management.
As we anticipate more changes to the Australian privacy landscape, it is helpful to reflect on what we can learn from other jurisdictions around the world.

A matter of trust

Cyber incident communications and reputation management

A reoccurring theme throughout the Cyber Summit was the importance of communications in a crisis, and how reputational damage caused by a cyber incident can linger long after the servers are back up and running.

Our 'Matter of Trust' panel – including leading issues management expert Sue Cato, Government relations advisor Jody Fassina, and Clyde & Co partner and panel moderator Reece Corbett-Wilkins – have all been on the frontline helping clients manage reputational risk through a cyber crisis.

In a fitting end to the Summit, they shared invaluable insights on how being well prepared and able to communicate with transparency and integrity can drastically transform how a cyber incident plays out with stakeholders, the Government, and the media.

Be prepared

There's no questioning that cybercrime is one of the biggest threats facing companies around the globe, but many entities are still under-prepared for a potential attack.

"*Every board in last six months has put a new item on their agenda – cyber risk. But there are a lot of boards who are just ticking boxes; they're not actually living it*," Sue Cato told the panel.

"*My firm ran two major cyber crisis planning scenarios in the same week. Both companies had crisis management plans an inch thick; one of them had learnt it and understood it, and the other had it in the bottom of the draw and had to start from scratch.*"

Board dynamics or company structures can also have a huge impact on how a crisis plays out, especially when you've got big personalities in the room.

Sue Cato emphasised the need for the 'war room' to be ready – know where your CTO is, who your back up CTO is in case they are not available at the time of an incident, and who your external facing spokespeople are.

In essence, Sue Cato highlights that you need to ensure your core team is ready and understands their role in an incident.

Build trust

Another key takeaway of the panel discussion was of course the importance of trust – and how companies need to build that trust, especially with Government.

"*It's not the case anymore of if you are going to be attacked or not, it is now a question of when. Thinking you can deal with a data breach in isolation, those days are gone*," Jody Fassina told the audience.

"Whether you like it or not, Government is now your partner. Get to you know your partner, talk to your partner, engage with your partner, be truthful to your partner. If you want help and assistance, engage with the government. When you look at a major breach, it's a no brainer that you've got to talk to Government, it goes to that fundamental, intangible quality which is so easily lost and hard to gain – trust."

So, what about when it goes wrong?

For Jody Fassina the key question to ask is why trust is missing and address that first. In particular, Jody Fassina urges entities to consider the Government as their partner and not the enemy.

And, of course, don't blindside them. "*Trust is a word, but so is surprise*," added Sue Cato. "*What people don't want, whether it's the Government or your stakeholders, is surprises.*"

Jody Fassina also warned of the likely response if companies fail to engage with government. "If they cannot trust you, you are going to see a plethora of legislation to say what you can and can't do."

Find the balance

The desire to be open and transparent can often conflict with legal advice placing entities in a difficult position when trying to navigate a cyber incident in a way that preserves goodwill. This is particularly prevalent in the early stages of an incident where the extent of access (if any) to personal information has not been assessed, but stakeholders want to know the answer.

"*Sometimes there's a difference between the legal advice and communications advice, there's maybe five percent we disagree on,*" Reece Corbett-Wilkins noted.

Sue Cato agreed: "*Ultimately corporations, or any entity, have to rely on legal advice, so generally the onus is on comms to be able to reach an understanding with the team of lawyers.*".

"*If the law says x, I see it as my job to see whether I am able to convince the lawyers on the five per cent. If I can't, I have to wear it and go in knowing what the implications are and make a risk-based decision.*"

Jody Fassina added: "*I understand that lawyers have an obligation to their client to give the best advice, but this is also about a social license. With consumer data you are a custodian, and you should never forget about that.*"

Be transparent

Another key stakeholder in any crisis is of course the media. "*It really helps if you already have a trusted relationship with the media, and that the media knows that you're telling them the whole truth,*" said Sue Cato.

"*Where reputation lives and dies is the surprise factor. If you're acting in a manner which is contrary to what people expect, if your media interactions are defensive and aggressive, it will start on a bad foot.*"

"*You should be able to demonstrate to the media that you actually want to engage with them as fully as you possibly can.*"

"*If the media thinks that this is a story that is worth chasing down, that's their job. If you can be straight-up with the media and answer as many of the questions you can, recognising that you want to get it right and not wrong, you'll find that's the way to take some heat out of it.*"

Jody Fassina added that getting it wrong can have more ramifications than just a bad article. "*If you aren't honest with what you do or don't know in a crisis, if the public pressure is out there, the Government will come out with a response, and you may not like it. Then you'll spend the next five to 10 years trying to unwind it,*" Fassina warned.

Key learnings

Be prepared - get your crisis comms plans ready and practice, practice, practice, until you know the plan inside out.

1. **Government is your partner** – deal them in quickly and don't hide information.

2. **Be transparent with the media** – they're just doing their job.

3. **Listen to your lawyers** – and your communications professionals – there is often a middle ground to be found if you work together.

4. **Start and end with building and maintaining trust** as the basis for all your communications, and you shouldn't go wrong…

Sponsorship partners

The Summit could not have been possible without the support and sponsorship from our conference sponsors.

PLATINUM

Gridware

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 cyberattacks out of our 24/7 Cyber Defence Centre. Our vision is to make Australia the safest country in the world to do business online.

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/

GOLD

Slipstream/Interactive

Slipstream is an Australian cybersecurity company, with world-class capabilities in Digital Forensics and Incident Response (DFIR), Active Defence and Assurance. With a national capability, Slipstream provides expert assistance to organisations across Australia and South-East Asia. Slipstream works closely with, and is a trusted partner of, insurers, brokers, legal teams and IT service providers ensuring victim organisations - small businesses through to large ASX-listed companies - manage and recover from cyber incidents.

Slipstream was acquired in April 2023 by Interactive, Australia's leading end-to-end technology solutions provider. Interactive delivers an integrated suite of managed and professional services to customers, including cyber security, multi-cloud, data centres, business continuity, network services and hardware maintenance. Interactive scales Slipstream's DFIR first responder capability, providing on-site assistance for victim organisations across Australia's capital cities and regions, creating a unique offering among Australian DFIR practices.

P: 1300 669 670

W: https://www.interactive.com.au/

McGrathNicol & S1

McGrathNicol is a specialist advisory and restructuring firm committed to helping business of all sizes improve performance, manage risk, and achieve stability and growth. The business landscape is always evolving, and we are here to help organisations leverage today's opportunities and anticipate tomorrow's challenges. With over 350 independent experts, our firm has built a reputation for delivering results for some of Australia and New Zealand's best corporations.

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 cyber criminals. We provide specialist knowledge and experience to help organisations build and maintain their cyber resilience and respond in the event of an incident.

P: +61 2 9338 2600

W: https://www.mcgrathnicol.com/

SILVER

Crowdstrike

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint and workload protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints and workloads on or off the network.

Learn more: https://www.crowdstrike.com.au/services/law-firms-and-insurance/

CTRL Cybersecurity

ASX 100 and Fortune 500 companies trusted information security partner. By embodying a forward-thinking mentality and a hyper-focused approach to organisational cyber risk profiling, CTRL implements tailored strategies to align cybersecurity with business objectives.

Driven by the mission to Pioneer Australia's Transition to Cyber Excellence, CTRL's team of highly specialised security experts are at the forefront of cyber, technology, and business operations; placing CTRL in a unique position to deliver innovative and effective solutions. CTRL remain a pure-play cybersecurity company. Proudly 100% Australian-owned and operated.

Empower. Elevate. Excel.

E: info@ctrl.co

W: https://ctrl.co/

Triskele Labs

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

We care and continually improve to deliver whatever it takes, and our customers know the difference. Our approach to exceeding expectations and delivering tailored services is truly one of a kind.

Our team goes the extra mile to demystify cybersecurity, develop customised programs, deliver on your specific needs to meet your budget and become your trusted partner.

P: 1300 24 Cyber

E: info@triskelelabs.com

W: https://www.triskelelabs.com/

BRONZE

KordaMentha

KordaMentha is an independent advisory firm providing specialist cybersecurity, financial crime, forensic, performance improvement, real estate and restructuring services across Asia-Pacific. Since 2002, our experts have been entrusted with some of the region's most complex and sensitive commercial situations.

P: +61 2 8257 3000

E: info@kordamentha.com

W: https://kordamentha.com/home

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/

Norton Lifelock Gen Digital

Norton empowers people and families around the world to feel safer in their digital lives, so you worry less about the darkness of cybercrime. Whether it's protection for your devices, online privacy, identity, or everything all-in-one, we make it easier to keep your digital life safer. Opt-in to cyber safety.

LI: linkedin.com/GenDigital

Logicalis

We are Architects of Change™. We help organisations succeed in a digital-first world.

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.

P: 1300 724 745

W: www.au.logicalis.com

Authors

Reece Corbett-Wilkins
Partner
Reece.Corbett-Wilkins@clydeco.com

John Moran
Partner
John.Moran@clydeco.com

Richard Berkahn
Partner
Richard.Berkahn@clydeco.com

Stefanie Luhrs
Partner
Stefanie.Luhrs@clydeco.com

Alec Christie
Digital Risk Partner
Alec.Christie@clydeco.com

Chris McLaughlin
Cyber Risk Advisory Principal
Chris.Mclaughlin@clydeco.com

Heasha Wijesuriya
Associate
Heasha.Wijesuriya@clydeco.com

Andrea Mitchell
Special Counsel
Andrea.Mitchell@clydeco.com

Jacky Li
Senior Associate
Jacky.Li@clydeco.com

Stuart Lloyd
Senior Associate
Stuart.Lloyd@clydeco.com

Hannah Stacey
Associate, Sydney
Hannah.Stacey@clydeco.com

Suzannah Hills
Communications Manager, Cyber
Suzannah.Hills@clydeco.com

Laurien Hush
Senior BD Manager
Laurien.Hush@clydeco.com

Michelle Nisbet
BD Executive
Michelle.Nisbet@clydeco.com

Aimee Johnstone
Client Executive
Aimee.Johnstone@clydeco.com

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.