Clyde & Co
Level 15
333 George Street
Sydney NSW 2000
Australia
Telephone: +61 2 9210 4400
Facsimile: +61 2 9210 4599
www.clydeco.com

By Email: cisgcomms@homeaffairs.gov.au

Cyber and Infrastructure Security Group
Department of Home Affairs
GPO Box 9984
Sydney NSW 2001

Our Ref	Your Ref	Date:
Cyber Strategy Submission 2024	Australian Cyber Security Strategy: Legislative Reforms Consultation Paper	1 March 2024

Dear Sir/Madam

Re: Clyde & Co's Submission to the Cyber and Infrastructure Security Group (CISG) on the proposed changes outlined in the Australian Cyber Security Strategy: Legislative Reforms Consultation Paper

1 Introduction

1.1 Clyde & Co is grateful for the opportunity to provide its insights into the evolving cyber threat landscape, and its support of legislative measures aimed to strengthen Australia's resilience to cyber risk.

1.2 We commend the Government for its continued commitment to addressing cyber risk at an aggregate level. This includes introducing new legislation to support victim organisations of cybercrime through information sharing, while balancing concerns around increased accountability and legal liability for cyber security events.

1.3 Our Submission is based on the findings of Clyde & Co's 'Under the Hood' Guide (titled **Under the Hood: Unveiling the cyber world through the eyes of an incident responder**) and the learnings generated by Clyde & Co's Cyber Summit 2024 and post-Summit Report. You can find our post-Summit Report and a copy of our 'Under the Hood' Guide here.

1.4 We hope that these resources provide the Government with valuable insight into the current views of the community, as well as actionable data that shines a light on the threat landscape which can inform public policy decisions.

1.5 Should the CISG wish to contact us for more information separately we would be pleased to provide further assistance.

2 Clyde & Co: Who we are and what we do

2.1 Clyde & Co is a multi-jurisdictional law firm offering specialist legal services across over 60 offices globally. Clyde & Co established its presence in Australia eleven years ago with expertise in core practice areas such as technology and privacy risk, underpinned by our speciality insurance experience.

2.2 In 2014, we established a cyber 'incident response' practice in Australia to service the cyber insurance market and their policyholder clients – to be a first point of call to help insured and uninsured entities respond to cyber incidents and data breaches. We act for a broad range of victims – SME organisations, large ASX listed corporates, local councils and other government agencies, as well as individuals (on a pro bono basis).

2.3 While we are a law firm and provide legal and regulatory advice relating to incidents, primarily our service offering is to act as 'incident response management' or 'breach coach'. In that role, we guide entities through various types of incidents from first awareness to resolution. We also have a specialist crisis communications and threat intelligence team.

2.4 Depending on the incident and needs of the impacted entity, we help co-ordinate the engagement of our fully screened panel of 80+ vendors[1] to ensure the entity receives help. As required, we also liaise with government agencies (such as the ACSC, CSRCU) for assistance.

2.5 In Australia, we have assisted on over 3,000 incidents during this time and globally over 5,000. This provides us with a range of experience of different incident types through this period, including BEC, ransomware, third party breach, extortion, insider threats, various types of data breaches, nation state and pure fraud related matters.

2.6 On 15 February 2024, Clyde & Co hosted a Cyber Summit for over 1,000 attendees and launched our Under the Hood Guide, which provides a deep dive on the key incident trends across various incident types. The audience members comprised of the cyber insurance industry, corporate and SME entities, regulators, the infosec community and incident response profession.

2.7 The Summit was designed around the '6 Shields' and generated discussion around issues, the subject of the Strategy generally and specifically the issues being considered in this round of consultation with the CISG.

3 Submission to the CISG on the proposed changes outlined in the Consultation Paper

3.1 We **enclose** the following documents:

(a) Clyde & Co's 2024 'Under the Hood' Guide; and

(b) Cyber Summit 2024 – Report.

3.2 In preparing our 'Under the Hood' Guide, we were motivated to achieve the following important goals:

[1] Ranging from network security, digital forensics, dark web monitoring, threat intelligence, ransom payment, ransom negotiation, data recovery, e-discovery / data cataloguing, public relations, communications, call centre, credit monitoring and ID protection, and counselling service providers.

(a) **Increase information sharing and mobilise collective action**

The private sector, incident response industry and government have a real opportunity to work better together to share information and actionable intelligence pre, during and post breach.

Working together under a common goal, combining resources in the right way can more effectively mitigate the initial impact and spread of incidents particularly those of a national significance or where multiple stakeholders are involved in consequence management.

Information can also be shared outside the context of supporting the immediate response of a specific incident, to sharing broader lessons learned to help others protect against further activity and consequence management.

However, clear rules of engagement and legal protections need to be in place to work as intended. There also needs to be an efficient means of sharing information in a sequenced way to ensure that the mission critical information (IOCs, TTPs etc) is shared in the early stages (say first 72 hours), versus broader lessons at later stages in the incident.

Further, there should be options to participate in some level of information sharing initially without committing to sharing all aspects of the incident (i.e. attack vectors vs ransom payments vs data privacy considerations).

(b) **Spotlight the cyber insurance industry as a key part of the solution**

The global cyber insurance industry has been at the heart of supporting clients uplift their cyber security controls and decisively respond to cyber incidents for over 15 years. Cyber insurers take on cyber risk the world over, and through brokers acting as risk advisors are committed to driving down cybercrime.

However, the cyber industry in Australia is underutilised, and more needs to be done to promote cyber insurance purchasing particularly for the SME sector which makes up 90% of businesses in our economy.

For example, it is estimated that only about 10% of SMEs purchase cyber insurance and are therefore not able to leverage the vast resources and expertise of the cyber insurance industry to protect them and help them respond. Those without cyber insurance aren’t typically able to take the necessary steps required of them to properly respond to cyber incidents – for example conducting detailed forensic investigations and conduct data reviews and notification campaigns to a large cohort of affected individuals.

Some industries are for example more at risk than others – NDIS providers, health service providers, real estate agents / conveyancers, and small professional services providers (such as law firms, accountants, financial advisors etc) are common examples of industries which need additional support based on the data they hold and risk of targeted financial crime (BECs / invoice fraud etc).

There is a lot of positive change that will occur if the cyber insurance market is better tapped into as a force multiplier. Organisations can transfer risk away from their bottom line, and through the insurance purchasing process can bolster their security controls, awareness of risks, and response capabilities, to drive wholesale improvements across the economy.

(c) **Small business focus**

As a nation of small businesses, we need to work together to support the heartbeat of our economy to adequately protect against cyber risk.

Free resources, centralised reporting frameworks, and playbooks will help reduce burden, but will only go so far.

Harnessing the trickledown effect of minimum-security requirements through supply chain contracting, industry focussed approaches to uplifting cyber security, and mandating cyber insurance through supply chains will also assist.

(d) **Spotlight third party breaches**

Third party breaches are where the risk sits and is a risk that proposed amendments to the SOCI Act have recognised and seeks to address by introducing more stringent security controls through service providers of critical infrastructure providers.

Multi-party data breaches which grip entire industries at once are a contemporary risk facing multiple industries. Parties involved in breaches (and their advisors) have an opportunity to work better together under a common goal to better respond and protect against misuse of data. This is something that the industry has been focussing on over the past few years since the NDB Scheme came into force.

Equally, more work can be done pre-breach by entities and their suppliers in terms of setting breach response expectations, confirming security compliance on an ongoing basis, and deleting data regularly.

(e) **Encourage a multi-disciplinary approach to cyber risk**

Within organisations, there continues to be an opportunity for cyber risk to be approached on a multi-disciplinary basis. As evidenced by the profile of Summit attendees, we are now seeing representatives from Legal, IT, Risk, Insurance, Comms, and Boards take an active interest in this area.

This should continue to be encouraged, particularly by Government, in driving skilled migration to attract diverse talent and by tertiary education in building a workforce ground up across technical and non-technical disciplines.

Cyber Summit 2024 – Report

3.3 On 15 February, Clyde & Co hosted the Cyber Summit 2024.

3.4 Using the Federal Government's Cyber Security Strategy 'cyber shields' to inspire the Summit agenda, we placed an investigative lens over these goalposts and interrogated how they can help drive positive change, while also addressing the potential downfalls and difficulties that could be faced along the way.

3.5 We brought clients, regulators, Government and the cybersecurity and insurance industries together to unpack how the Cyber Security Strategy and the proposed regulatory change could help pave the way to establishing Australia as the most cyber secure nation by 2030.

3.6 We captured the views of the community on the day and generated the findings in the **enclosed** post-Summit Report.

3.7 We draw your attention to pages 25 – 27 of the Cyber Summit 2024 Report, which details the results of live polling of attendees on the day, covering topics such as: "*What is the* *most effective way for Government to reduce cyber-attacks?*” and “*Should organisations be required to share information about ransomware attacks with the Government?*”.

4 Conclusion

4.1 We hope that the findings from both the ‘Under the Hood’ Guide and the post-Summit Report are of use to the CISG, and we commend you for your hard work to bolster the nation’s cyber resilience.

4.2 Let us know if you need anything else.

Yours sincerely

Clyde & Co

Reece Corbett-Wilkins
Partner
Clyde & Co
DDI: [redacted]
Mob: [redacted]
Email: [redacted]

Richard Berkahn
Partner
Clyde & Co
DDI: [redacted]
Mob: [redacted]
Email: [redacted]

John Moran
Partner
Clyde & Co
DDI: [redacted]
Mob: [redacted]
Email: [redacted]

Stefanie Luhrs
Partner
Clyde & Co
DDI: [redacted]
Mob: [redacted]
Email: [redacted]

Clyde&Co One

Under the Hood

Unveiling the cyber world through the eyes of an incident responder

A deep dive in to:

- Ransomware
- Business Email Compromise
- Third Party Breaches
- Other Incident Types
- Claims trends

Foreword

Reece Corbett-Wilkins
Partner, Clyde & Co

John Moran
Partner, Clyde & Co

Richard Berkahn
Partner, Clyde & Co

Stefanie Luhrs
Partner, Clyde & Co

With the recent release of the 2023-2030 Australian Cyber Security Strategy (**Strategy**),[1] there is a strong desire by government, service providers, industry, insurers, and the private sector to improve our nation's cyber posture and fortify our defences against cyber-attacks.

This includes reducing the overall attractiveness of the Australian market to cyber criminals and introducing deterrence and friction to their business model. Where incidents do occur, government and industry are exploring ways to better work together to limit the consequences of breaches on lives and livelihoods.

By providing our insights into the cyber incident landscape, we hope to provide the industry with useful datapoints to help drive the national agenda. In this Guide we draw from our in-depth incident response experience having supported thousands of clients over the past ten years when we started our journey as a team.

Not all these incidents hit the front page of the news – in fact most don't. But there are still countless lessons that can be drawn upon from every single incident, great or small, and we hope this Guide brings some of that to life.

While mid to large scale corporates make up the bulk of clients that we support, we also support small to medium sized enterprise (**SME**) (an organisation with no more than 500 employees) and micro-SMEs (with revenues <$3 million AUD annually). However, the industry needs to continue to break down the economic barriers preventing SMEs from obtaining support pre and post incident. We have a 'small business problem' on our hands, which will take time to solve.

In the meantime, the cyber insurance industry continues to focus on ensuring our digital ecosystem remains secure at all levels. Despite the immense protective value that the cyber insurance industry provides to policyholders, our economy is grossly underinsured against cyber risks. Further work is required to better promote the value of cyber insurance and its uptake to insulate our economy. Insurers play a vital role in supporting policyholders with uplifting their capabilities.

It's not just the private sector who are focussing on cyber risk enhancements. Government agencies across the Commonwealth, states and territories, and local council level are also looking to lead by example and manage their cyber risk profile in line with best practice and community expectations.

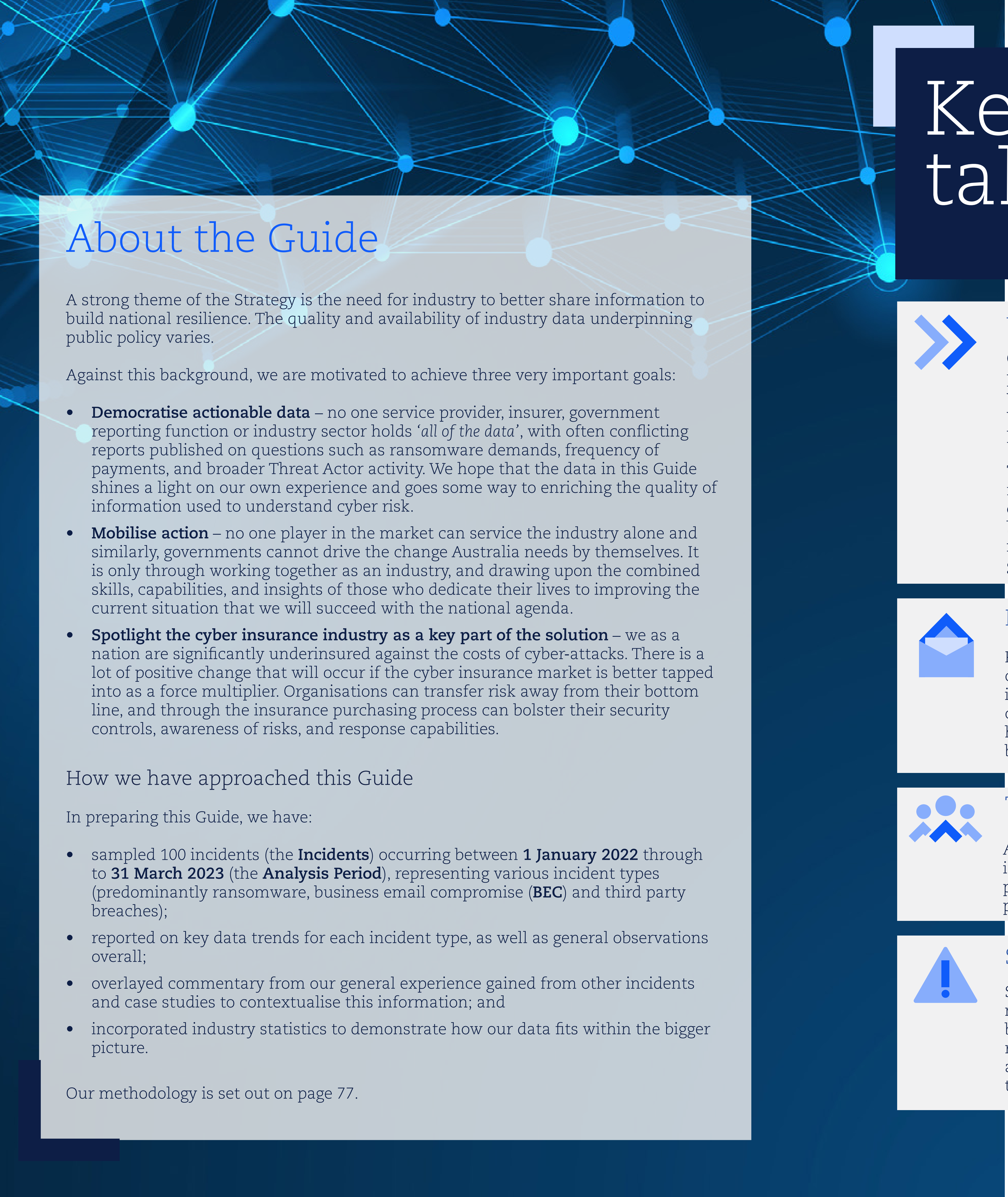
The recent introduction of the Mandatory Notification of Data Breach Scheme in New South Wales demonstrates a real desire to focus on this within government, requiring NSW agencies to operationalise breach response into the core of their crisis management capability. Over time, this will naturally drive investment in breach prevention.

While we do provide support with government agency breaches, the data in this Guide is largely informed by incidents impacting the private sector. That said, our insights are equally applicable to government teams (including local councils).

We expect the target audience reading this will be executive team members, Boards, insurance brokers and risk advisors. We also commend this Guide to anyone who is involved in making life harder for cyber criminals.

As many will attest, we are operating in a complex, fast evolving, and asymmetric environment where cyber criminals only need to get it right 1% of the time. The rest of us need to get it right 100% of the time.

We hope this Guide provides helpful information to take forward into 2024.



About the Guide

A strong theme of the Strategy is the need for industry to better share information to build national resilience. The quality and availability of industry data underpinning public policy varies.

Against this background, we are motivated to achieve three very important goals:

- **Democratise actionable data** – no one service provider, insurer, government reporting function or industry sector holds '*all of the data*', with often conflicting reports published on questions such as ransomware demands, frequency of payments, and broader Threat Actor activity. We hope that the data in this Guide shines a light on our own experience and goes some way to enriching the quality of information used to understand cyber risk.
- **Mobilise action** – no one player in the market can service the industry alone and similarly, governments cannot drive the change Australia needs by themselves. It is only through working together as an industry, and drawing upon the combined skills, capabilities, and insights of those who dedicate their lives to improving the current situation that we will succeed with the national agenda.
- **Spotlight the cyber insurance industry as a key part of the solution** – we as a nation are significantly underinsured against the costs of cyber-attacks. There is a lot of positive change that will occur if the cyber insurance market is better tapped into as a force multiplier. Organisations can transfer risk away from their bottom line, and through the insurance purchasing process can bolster their security controls, awareness of risks, and response capabilities.

How we have approached this Guide

In preparing this Guide, we have:

- sampled 100 incidents (the **Incidents**) occurring between **1 January 2022** through to **31 March 2023** (the **Analysis Period**), representing various incident types (predominantly ransomware, business email compromise (**BEC**) and third party breaches);
- reported on key data trends for each incident type, as well as general observations overall;
- overlayed commentary from our general experience gained from other incidents and case studies to contextualise this information; and
- incorporated industry statistics to demonstrate how our data fits within the bigger picture.

Our methodology is set out on page 77.

Key takeaways

We're heading in the right direction with ransomware

Overall, ransomware incident attack frequency is **down**, and ransom demand payment frequency is **down**, however ransom demand quantum is **up**. Less victims are paying, but if they do pay, it's for a higher quantum than ever before, with Chainanalysis reporting $1.1 billion USD ($1.68 billion AUD) in ransomware payments in 2023.

This means that while the industry is moving in the right direction to defend against ransomware attacks and resist the payment of ransoms (in Australia), we are not out of the woods yet. Threat Actors are fully funded. The significant payments being made today around the world will become our problem tomorrow. More work is required to maintain the downward trends, including further investment from government and law enforcement to disrupt cyber-crime syndicates.

Houston, we have a BEC problem

Perhaps due to the over focus on counter-ransomware measures, our economy continues to lose significant capital each year to Business Email Compromise incidents and associated Funds Transfer Fraud. The sums (inadvertently) paid to criminals each year far outweigh payments to ransom gangs (our estimate, some half a billion Australian dollars annually) and measures to prevent this loss need to be given equal priority alongside anti-ransomware initiatives.

Third party breach is the new ransomware

As a collective industry, this is where the risk sits. A rising tide lifts all boats, and industry leaders should look to raise the standards not just of their own security posture by example, but that of their entire supply chain. Recent large scale multi-party data breaches highlight the need for continued focus in this area.

Small business, big challenge

Small to medium sized incidents are where the volume of cyber incidents rest. We need to critically reflect on how to approach cyber security expectations of small businesses that are time poor, resource constrained and fly beneath the regulation radar. Educating and building awareness is one thing, but incentivising action is another. We are a country of small businesses, and our approach needs to address the collective mass.

There is some good news, amongst the constant cyber doom and gloom

With the constant change of pace from Threat Actors, cyber security enhancements, and regulatory uplift requirements, many are struggling to keep up with what's asked of them.

However, in recent years we have seen a real momentum for change – with a noticeable gear shift towards continuous improvement and top-down investment. Boards are well and truly aware of the need to support cyber risk strategies.

Beneath the surface, organisations are building team capabilities to protect and respond, harnessing experience of those from diverse backgrounds with both technical and non-technical qualifications.

Wherever you are on the journey, we hope that this Guide can help build momentum internally for creating change necessary to better protect your organisation from cyber risk.

Thank you and we look forward to working with you in 2024

There is a saying that we adopt internally: *'a year in incident response is the equivalent of dog years – seven years in the real world'*.

And for anyone that has been through an incident, you know what we mean.

The turbulence, pace of activity, and continuous troubleshooting and decision making required to respond to emerging challenges sees months pass by in a blink. The human toll on incident response teams, frontline staff, and the community is real, but so too is the reward of knowing you made a difference.

Thank you to those who dedicate their working lives to address this risk head on.

We applaud the Australian Government's bold and ambitious approach in developing and driving the Strategy, and we look forward to living in a world where Australia can hold its head up high as the most cyber secure nation in 2030.

A big thank you to the Oracle team

In mid last year, we set out on a mission to create this Guide. It has been something we have wanted to do for a very long time and are grateful for the chance to give back to the industry.

Like any major project there are many unsung heroes and we want to thank everyone for their contribution to pulling this together.

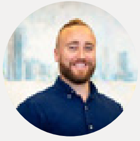
We want to thank the Oracle team who have worked on the Guide:

- Caitlyn Bellis
- Mohammed Abuwala
- Clementine Wilkie
- Annabelle L'Estrange
- Georgia Schulberg
- Alex McGuire
- Aimee Johnstone
- Linda Tran
- Sofia Xu
- Laurien Hush

We also want to thank Coveware and others from the industry who have contributed to its shape and direction.

We hope it provides a useful conversation starter throughout 2024 and beyond.

John Moran
Partner, Sydney
[redacted]



Reece Corbett-Wilkins
Partner, Sydney
[redacted]

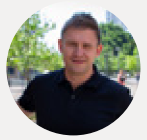
Richard Berkahn
Partner, Sydney / Auckland
[redacted]

Stefanie Luhrs
Partner, Brisbane
[redacted]

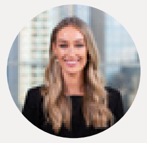
Alec Christie
Digital Risk Partner, Sydney
[redacted]

Andrew Brewer
Director, Cyber Risk, Brisbane
[redacted]

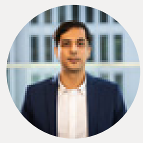
Chris McLaughlin
Cyber Risk Advisory Principal, Sydney
[redacted]



Richard Martin
Director Communications, Cyber, Sydney
[redacted]



Caitlyn Bellis
Associate, Sydney
[redacted]



Mohammed Abuwala
Cyber Threat Analyst, Sydney
[redacted]

Contents

Deep Dive Topic 1: Ransomware

Ransomware

What is ransomware?

We have all become accustomed to this incident type, but it's worth going over the history.

Put simply, ransomware describes the process where a third party deploys malicious code (malware) across a network to lock up (or 'encrypt') data stored within it. Generally, this data is not able to be 'decrypted' without the use of a decryption key.

Without viable (recent) backups, organisations are typically held hostage to Threat Actors, forcing them to consider paying a ransom demand to obtain a decryptor and recover data. This is where the pressure starts to mount, with many organisations facing data loss or system inoperability as the only alternative.

Over the years, ransomware has become a widespread tool of choice for Threat Actors seeking to extort victim organisations for payment. Before 2020, ransomware was common, but we did not see anywhere near the eye watering ransom demand sums that hallmarked the years from 2020 to 2022.

Previously, many organisations paid ransoms (1-2 BTC) and moved on with little afterthought. Much of the industry was focussed on data recovery solutions.

Big Game Hunting and double extortion tactics

In late 2019, Threat Actors significantly upped the ante and engaged in 'big game hunting'. This involved conducting incredibly sophisticated and targeted attacks against large well-known brands with a reputation to protect.

In addition to encrypting systems, Threat Actors began to recognise that taking data on their way out of systems was a way to increase their leverage during the ransom negotiation process. This tactic, known as 'double extortion', surfaced in Australia in late 2019 / early 2020, prior to the Covid-19 pandemic, although gained significant prominence in the months and years that followed.

Essentially, if a settlement cannot be reached, the Threat Actor will typically stage the victim organisation's name on their Data Leak Site (a website accessible through the dark web) before leaking the stolen data online.

With mainstream media closely following these dark web Data Leak Sites, Threat Actors know how to expose just enough information to ensure a publicity event without throwing away all their leverage at once. Media outlets (including cyber security trade publications) suddenly became the mouthpiece for Threat Actor behaviour and an unofficial member of the extortion eco-system.

It goes without saying that the publication of data can have a significant impact on an organisation from both a reputational and legal perspective. There is undoubtedly a human impact: even if data misuse does not occur (say ID theft) the alarm and concern caused across the community from data breaches is a real risk. Every breach has the potential to erode the faith our community has in the digital eco-system.

Threat Actors know this and are often willing to do whatever it takes to generate adverse publicity to leverage payment or establish their credentials as a force to be taken seriously.

Threat Actors are also acutely aware of the legal frameworks and regulatory obligations that apply to organisations. Threat Actors often weaponise data protection laws to pressure victims into paying. This includes 'beneath the iceberg' issues such as retaining datasets over a lengthy period.

The irony of course, is that paying a ransom does not by itself extinguish privacy reporting obligations altogether for victim organisations. Threat Actors play on this fear, nevertheless.

Triple extortion tactics – a new face of ransomware extortion

In recent years, victim organisations have become better at restoring compromised environments from backups and withstanding the adverse publicity associated with data leaks. As a result, in addition to data extortion, Threat Actors have sought to increase their leverage even further.

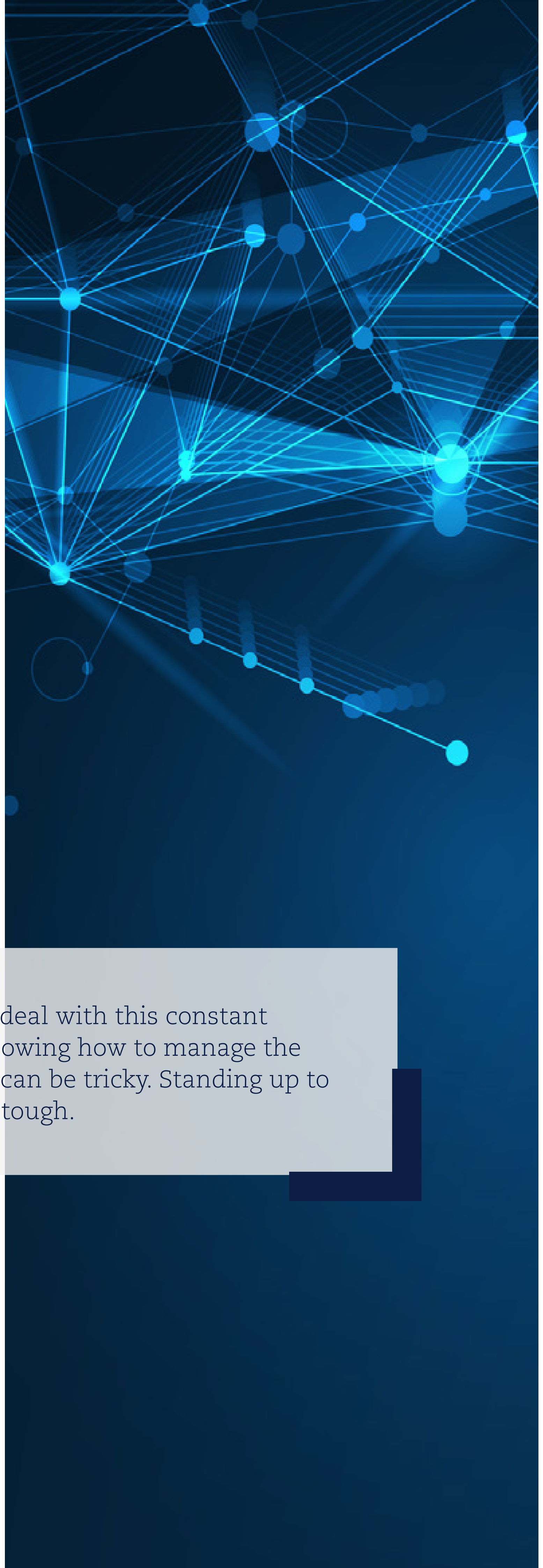
Nowadays, it is common for Threat Actors to undertake additional measures to intimidate and pressure victim organisations to reach a settlement and pay the demand – these actions and tactics are often referred to as 'triple extortion'.

Common examples of triple extortion include:

- issuing Distributed Denial of Service (**DDOS**) attacks against victims' websites to bring them down;
- emailing staff or contacting front of house (i.e. general office number/ reception);
- contacting directors and officers by phone/email/social media. In an example of how far Threat Actors will go, we saw a Threat Actor send a victim organisation's CEO flowers to their home address. We have also seen direct threats made to individuals (although thankfully not as extreme as some horrendous US examples where Threat Actors have threatened the personal safety of employees at home);
- contacting customers directly, seeking to extort them for the non-publication of their data (this is commonly known as 'secondary extortion');
- highly weaponising stolen datasets to target individuals or business-to-business (**B2B**) customers of the victim organisation, usually on the Threat Actor's Data Leak Site;

- infiltrating internal communications (such as Microsoft Teams) and monitoring other communications channels (such as email accounts);
- permanently deleting or manipulating datasets within the systems of the victim organisation;
- contacting the media or regulators directly (a recent US case involved a Threat Actor filing a breach report regarding the victim organisation to the the Securities and Exchange Commission); and
- on rare occasions, publishing a negotiation transcript online.

> For many organisations unprepared to deal with this constant barrage, the stress can be profound. Knowing how to manage the Threat Actor alongside everything else can be tricky. Standing up to this behaviour in the fog of war can be tough.



Data theft only extortion events – a highly effective tactic

In the past 12 months, we have seen a further evolution of Threat Actor tactics in the form of 'data theft only' extortion events. This is where the Threat Actor fails to deploy encryption malware before leaving the network, and rather focuses on taking a much larger volume of data with them on the way out.

A slight nuance to this is Threat Actors simply stealing data – which has been around for as long as cyber-crime has existed. The key differentiator here is whether the Threat Actor group runs a Data Leak Site or is simply motivated by taking data for sale and misuse.

Not all Threat Actors run a Data Leak Site. Where we refer to data theft only extortion events, we are generally talking about Threat Actor groups that will seek to extort a victim organisation as a quid pro quo for the suppression of a disclosure via their Data Leak Site.

There are multiple reasons why Threat Actors have evolved in this way. Whether it's due to the pressure to get out of an environment without being caught, a lack of willingness to provide after sales tech support, or a ransomware-as-a-service (**RaaS**) team that isn't well co-ordinated – either way, this recent trend is highly effective.

They may also be hedging their bets that a victim organisation will be more likely to pay on the basis that the event can be managed quietly. Once a system is encrypted – it often leads to operational disruption requiring the victim organisation to communicate the incident to staff at a minimum, and often external stakeholders too. In some circumstances, this could lead the victim organisation to become less willing to pay on the basis that the event is already in the public domain.

Either way, the psychology and pressure tactics of Threat Actor behaviour is highly sophisticated.

It is also important to note that where we would previously see gigabytes of data stolen (100,000s of documents) we are now seeing terabytes of data being stolen (millions of documents). Often these are taken from multiple locations across a network, with a random sampling of data taken from each source location (a little bit from here, a little bit from there) to keep victim organisations guessing.

Practically, this means that in assessing potential data risk exposure, victim organisations must cast the net wide and assume breach for a much larger dataset than what was likely taken (albeit accessed by the Threat Actor as part of their overall activities). Without forensics to pinpoint what was actually accessed and taken, victims are left with limited options – to engage with the Threat Actor for answers, brace for a data publication event to confirm what was stolen, or face the real prospects of notifying a much larger cohort than might be required, in the intervening period.

Threat Actors know this. Their business model is carefully crafted in a way that imposes pressure on victim organisations to consider buying back the certainty of the unknown. The goal is to ultimately corner victims so they feel no choice but to suppress the publication of large and complex datasets that could otherwise cause reputational and legal risk.

This is a key focus of the Strategy, additional Department of Home Affairs initiatives and the industry counter-ransomware focus; to create a norm of victim organisations being less likely to pay in spite of all of the circumstances at play. However, class actions and regulatory investigations risks remain, and Threat Actors will continue to leverage this where they can.

With this background, let's dive into the data.

How big is this problem?

Ransomware remains a prevalent form of cybercrime impacting Australian businesses.

From our own stats, ransomware incidents accounted for **37%** of total event types over the Analysis Period. Around the same period, the following was reported by other bodies:

- Between July 2022 to December 2022, the OAIC reported that **29%** of all data breaches resulting from cyber security incidents resulted from ransomware[2]. Between January 2023 and June 2023, the OAIC reported 53 notifications related to ransomware, making up **31%** of incidents reported during this period.[3]
- Between July 2022 and June 2023, the European Union Agency for Cyber Security (**ENISA**) reported that ransomware made up the majority of their incidents during this period, at **31.2%** of incidents.[4]
- The lower volume of ransomware reporting is also noted in the Information Commissioner's Office (**ICO**) **June 2021** and **March 2022** report, which states that ransomware made up less than **8%** of the data breaches reported for that period.[5]

Interestingly, the Australian Cyber Security Centre (**ACSC**) reported considerably lower rates of ransomware incidents. Between July 2021 and July 2022, the ACSC reported it responded to 135 cyber security incidents 'related to ransomware', representing only **10%** of the total 1,100 cyber security incidents responded to.[6] The following year, between July 2022 and June 2023, the ACSC reported the same percentage of incidents relating to ransomware.[7]

The significantly lower volume of ransomware incidents reported to ACSC indicates that ransomware incidents are underreported. It suggests that the ACSC is mainly being used to report other incident types such as phishing, scams and business email compromise.

Either way, ransomware incidents make up a large piece of the incident pie.

How does this compare over the years?

In 2020 and 2021, ransomware saw a sharp uptick both in Australia and globally. We have used 2020 as the baseline for our four-year comparison, being the highest volume of ransomware incidents for our practice.

2022 and 2023 saw a downtick in the volume of ransomware incidents, as compared to 2020 and 2021. This is good news and is likely due to a combination of factors including increased investment in security controls to mitigate against ransomware attacks and enhanced early detection and response capabilities.[8]

Under-reporting is another real possibility, but we have assumed that there is a level of under-reporting across all years.

Stepping back a bit, and comparing the Australian experience to overseas, what we saw in 2022-2023 (i.e. the Analysis Period) was a national awakening in the US about the prevalence and impact of ransomware following major events and this becoming a front-page news / top of the Board agenda item.

Speaking with expert cyber extortion incident response firm, Coveware, through this period Australia lagged slightly behind the US in terms of national reckoning following the Colonial Pipeline attack, but we quickly followed suit having experienced major events in our own jurisdiction. We could no longer pretend that this issue was one impacting large US companies only (despite the majority of ransomware incidents still occurring in the US).

Despite this, industry experts continue to express concerns about Australian organisation's apparent lack of preparedness to counter these sophisticated hacks, jeopardising the security of personal information belonging to Australians.[9]

The need to take further wholesale action is clearly still required and is something the Strategy is keen to address.

> *'A string of high-profile cyber events in Australia in 2022 provided a strong catalyst for change, including substantial investments to fortify cybersecurity measures, address vulnerabilities and bolster the resilience of Australian organisations against the evolving threat landscape. This proactive approach reflects a global trend in recognising the urgency of cybersecurity enhancements.'*
>
> **Coveware**

Four years of ransomware – a longitudinal view

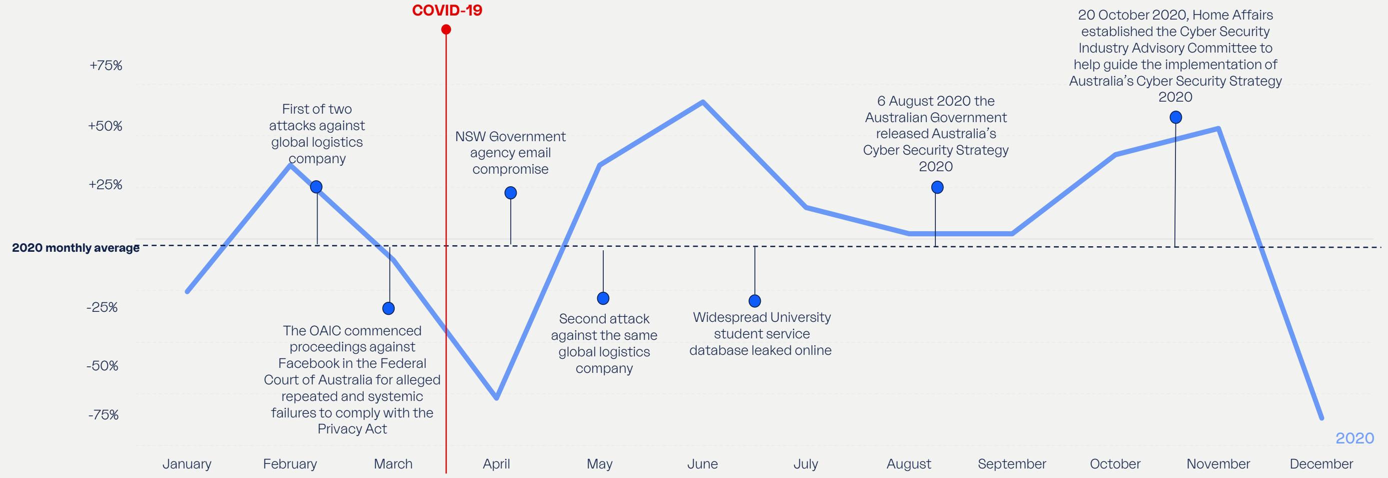
To demonstrate the above, we have mapped out four years of 'ransomware' engagements which have the hallmarks of precursor activity or confirmed system breaches, using 2020 as a baseline for comparing 2021, and 2022-2023.

We have included in the count confirmed 'ransomware', 'extortion only data theft events' and 'network compromise events', irrespective of whether we were able to determine the Threat Actor behind the attack, and irrespective of whether they are linked to a ransomware-as-a-service (**RaaS**) group which runs a data leak site. In other words, this includes incidents where the Threat Actor was caught very early in the act before taking data or encrypting systems (which we appreciate, aren't strictly ransomware events) to demonstrate the breadth of this type of activity.

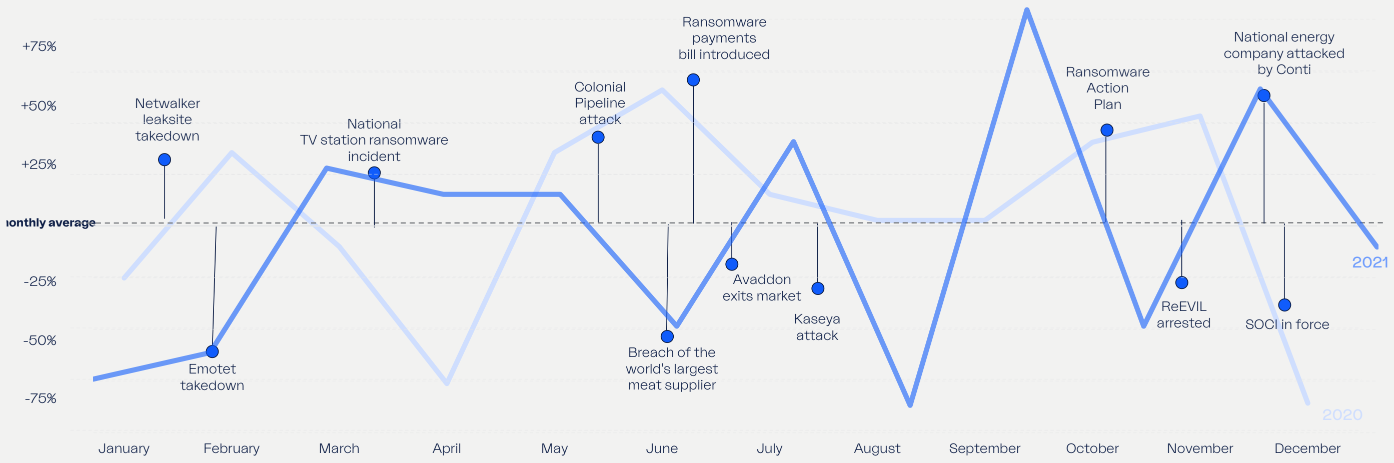
This does not include events where vulnerabilities were present but not exploited (such as Log4j which required whole of industry patching) or where Threat Actors were tapping at the door but there was no system access (which occurs millions of times per year across environments).

We have also only counted 'multi-party-data-breaches' once, even if we were engaged to act for multiple clients of the breached entity (i.e. it is counted as one event only).

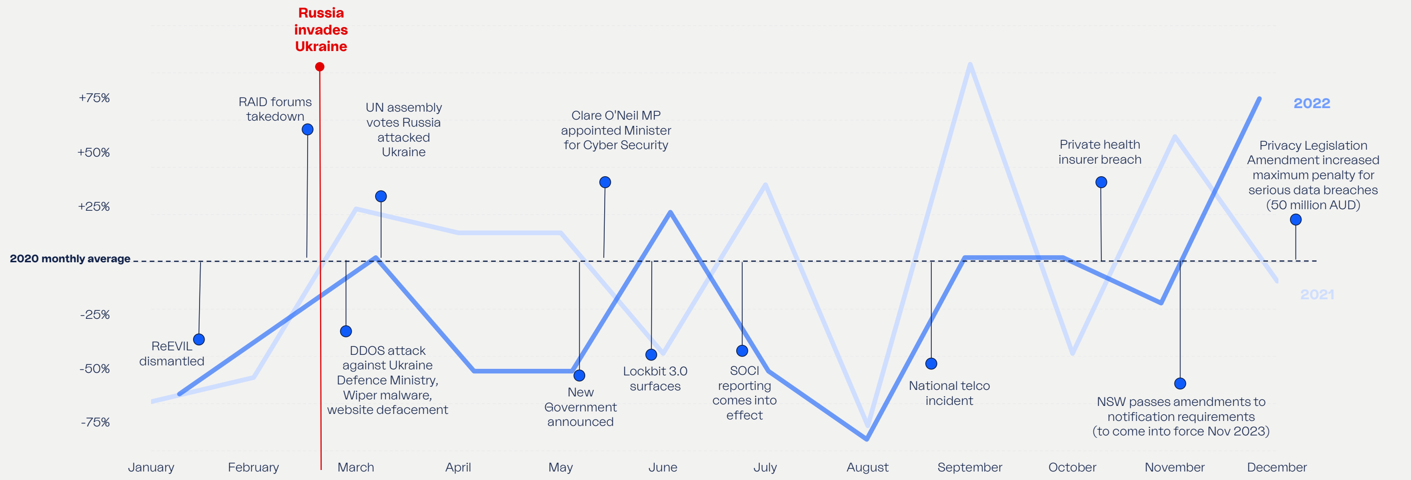
Ransomware trends in 2020



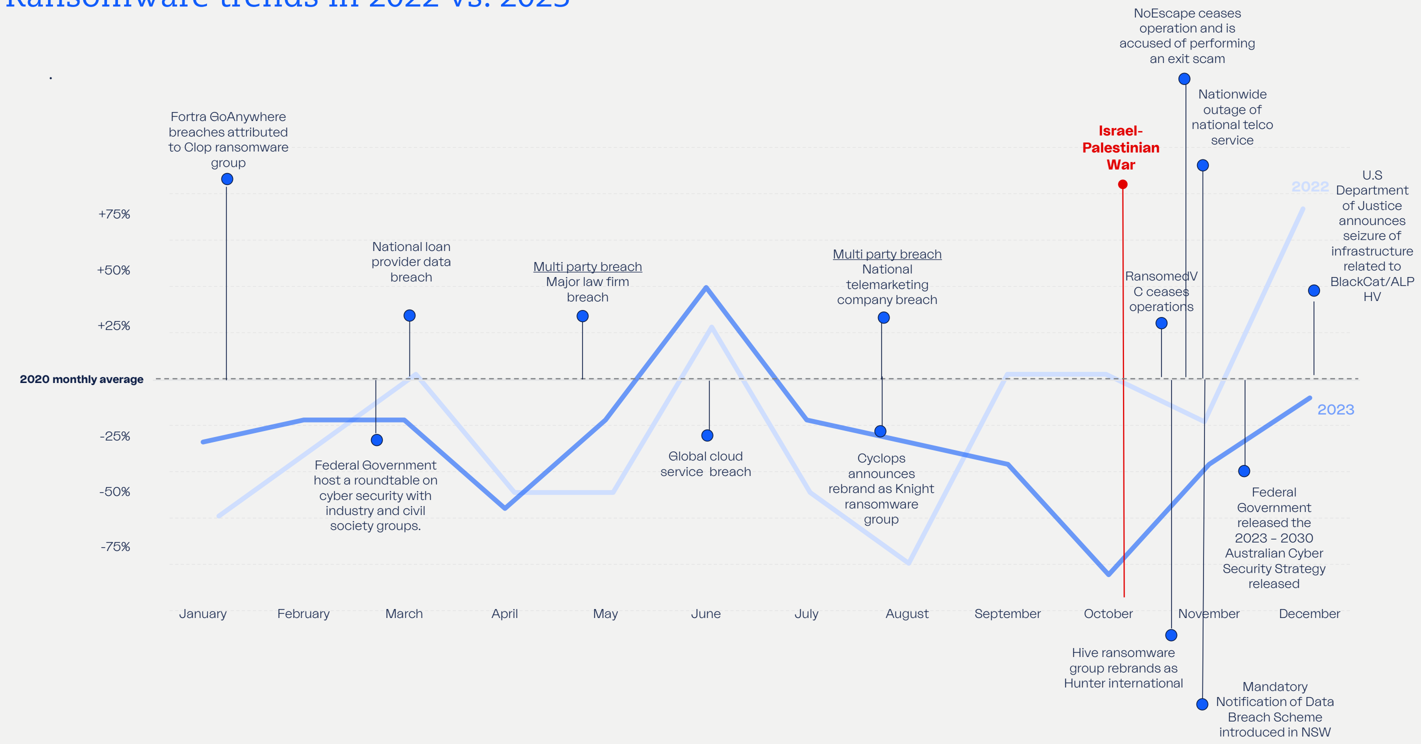
Ransomware trends in 2020 vs. 2021



Ransomware trends in 2021 vs. 2022



Ransomware trends in 2022 vs. 2023



What can we learn from this?

Our data and experience paint an interesting picture of various developments in Threat Actor behaviour and trends across the past four years. If we could take away just one headline it would be that Threat Actors are incredibly agile and persistent in their modus operandi.

It's also clear that there are cycles of activity and inactivity, driven by holiday periods, law enforcement takedowns, and in-fighting and fragmentation from Threat Actor RaaS groups.

Overall, it is pleasing to see a general downward trend of ransomware attacks since the 2021 peak which is something we explore further in this Guide.

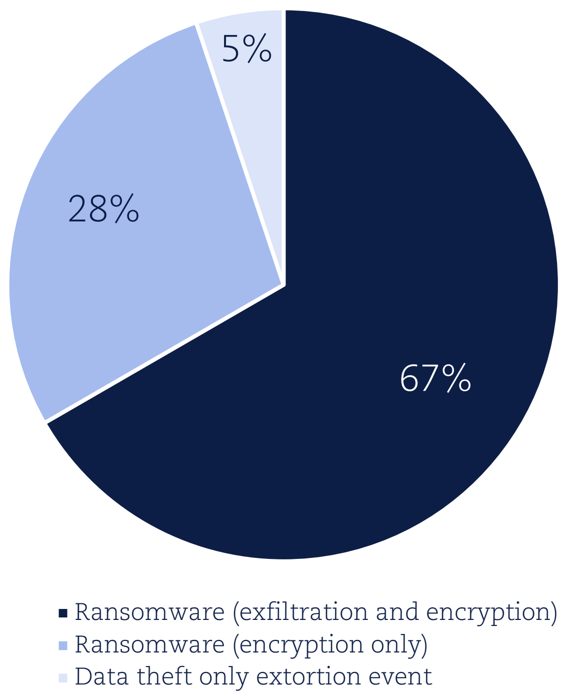
Key finding 1: **Data extortion on the rise**

It is clear to see that the ransomware business model has evolved over time.

1. Time and time again we see that when Threat Actors identify potential hurdles or experience disruption to their usual attack flow – i.e. organisations becoming increasingly cyber resilient – they pivot their strategies to remain relevant.
2. The rise in data theft only extortion events, and decline in encryption is a perfect example. That said, as evidenced below, encryption events remain prevalent. On the flip side, there are also cases in which encryption has occurred, but no data was taken.

Relevantly, this trend of data theft only extortion events has become more common throughout mid to late 2023 (being outside the Analysis Period) – therefore, while it only represents a small piece of the pie in the Analysis Period, we consider these proportions have shifted already (and will continue to).

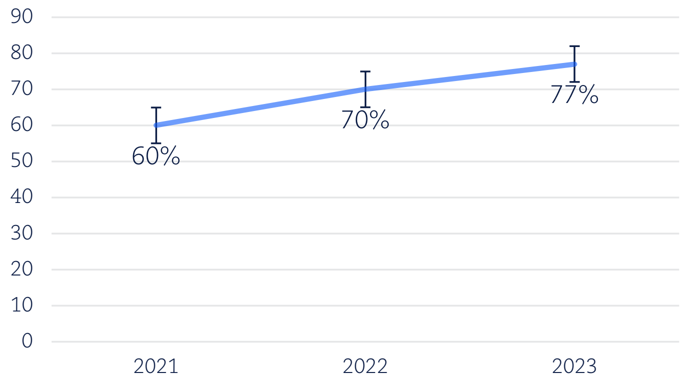
Ransomware Incident Sub-Types



In the context of extortion, the data shows that over the past few years, there has been a clear trend towards data exfiltration as a favoured double extortion tactic. To put it into perspective, data exfiltration was only confirmed in about **60% of cases in 2021**, increasing to **77% in 2023.** Overall, data exfiltration featured in almost **70% of all ransomware Incidents** during the Analysis Period.

We have overlayed our data with Coveware's data over the 2021-2023 period to complete the picture.

Yearly % of Ransomware Incidents Involving Data Exfiltration



The threat of exfiltration is not just a 'smash-and-grab' where a few documents are extracted from the victim's environment – the Australian Signals Directorate's (**ASD**'s) data indicates that between 1 November 2021 and 30 October 2022, the average amount of data reported to have been exfiltrated during a breach was around **120 gigabytes**, which could equate to hundres of thousands and potentially up to a million sensitive files.

Are Threat Actors bluffing?

When faced with a data extortion scenario, the first critical hurdle is to validate the threat.

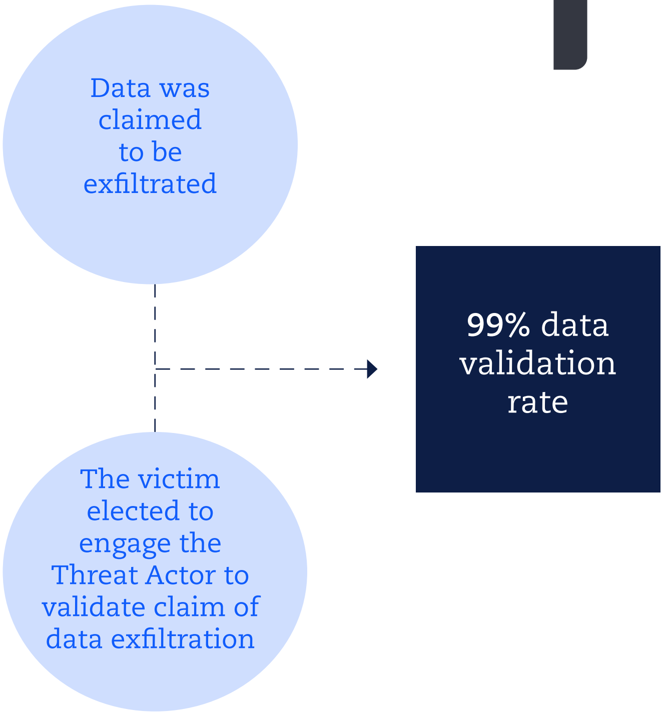
In other words, if a Threat Actor is claiming to have exfiltrated 100 gigabytes of data and threatening to publish that data online unless you pay them $1 million (usually in BTC/USD), the first point to validate is whether they actually have your data.

Often organisations will seek to answer this question of what, if any, data has been taken through completing a forensic investigation. However, forensic investigations regularly take several weeks to complete, and realistically, the impending threat of data being published means that victim organisations cannot afford to wait that long to determine data risk. There are also typically evidentiary limitations due to logging unavailability or anti-forensics activities of Threat Actors, that make it difficult (if not impossible) to forensically determine what information was accessed/exfiltrated.

In the absence of reliable forensic findings, one strategy often employed by victim organisations is to engage with the Threat Actor to validate their claim and determine what data may have been compromised. This can also help to create efficiencies in the investigation approach by narrowing the focus of the forensic investigation based on the source location of data stolen.
So, how often are the Threat Actors telling the truth, and how often are they bluffing? This question comes up in every engagement.

During the Analysis Period, we found that in 99% of ransomware incidents where the victim organisation asked the Threat Actor to prove what data they had taken, the Threat Actor was able to demonstrate they had taken some amount of data.

However, the question often remains as to whether they have in fact taken all of what they say they have.



Data was claimed to be exfiltrated

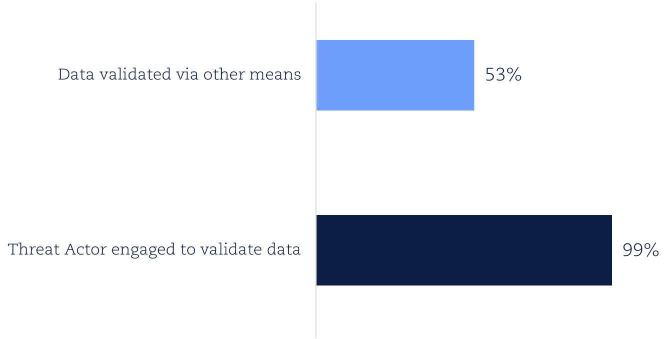
The victim elected to engage the Threat Actor to validate claim of data exfiltration

99% data validation rate

On the flip side, in cases where the victim organisation elected not to engage with the Threat Actor and instead rely on the forensic investigation to determine what data had been exfiltrated, we saw a significantly lower rate of validation (53%). In other words, in 53% of ransomware cases, the forensic investigation was successful in confirming what data was taken – this leaves a significant gap, with 47% of organisations not getting the answers they needed to adequately assess their data risk and potential exposure. Again, this comes back to evidentiary limitations making it difficult to determine what data (if any) was exfiltrated.

If we consider this in the context of the ransomware business model, it reinforces the notion that victim organisations are somewhat beholden to engage with Threat Actors to confirm their data risk exposure.

Data Validation Rates – Engaging Threat Actor vs Other means

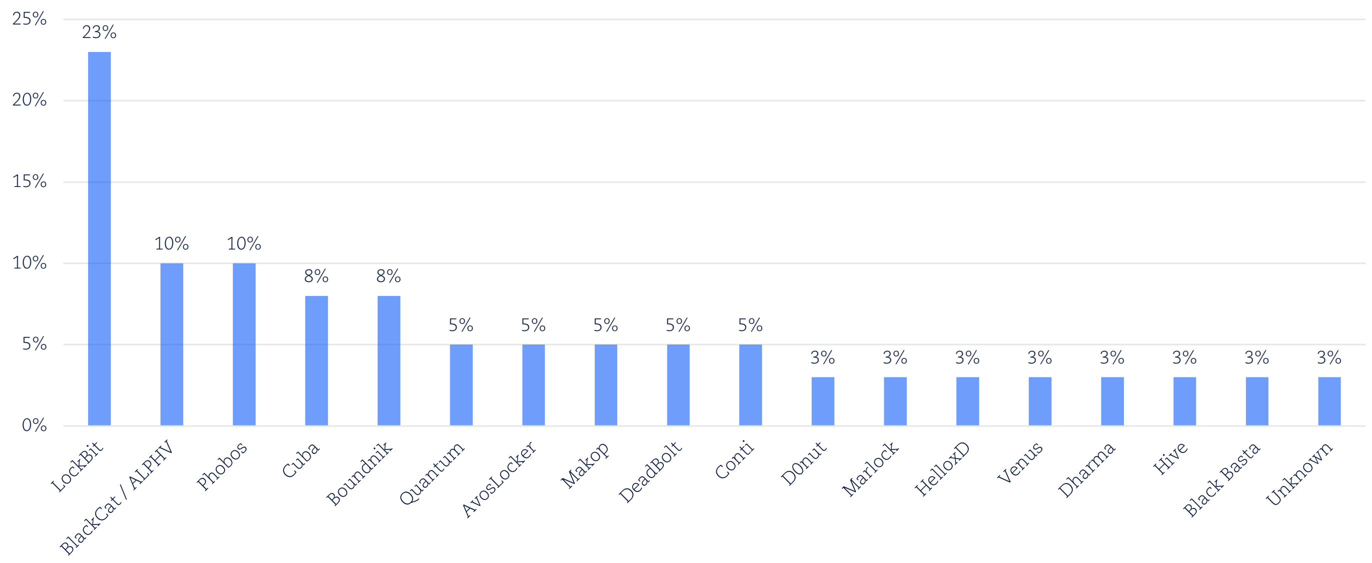


Key finding 2: **New kid on the block – Threat Actor group fragmentation**

The Analysis Period saw a huge spike in the utilisation of the RaaS business model and the number of corresponding Threat Actor groups.

The most active RaaS groups observed during the Analysis Period were LockBit and BlackCat/ALPHV. This is consistent with Coveware's data from the same period. LockBit also had the highest number of victims claimed on their Data Leak Site, as compared with other RaaS groups[10].

Most Observed Threat Actor Groups during Analysis Period



Pre 2020, we could list on just one hand the Threat Actor groups responsible for majority of the ransomware incidents that occurred in Australia.

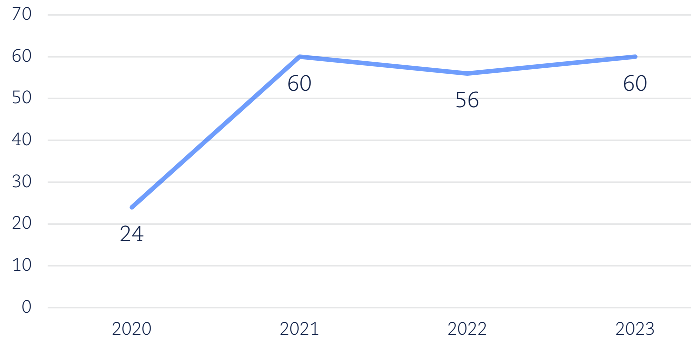
Since that time, there has been a major shift in the Threat Actor ecosystem as a result of increased scrutiny from law enforcement, the arrest of key cyber actors by the FBI and international law enforcement, and the introduction of various sanctions against specific individuals, countries and Threat Actor groups.

This, together with in-fighting, has collectively resulted in the fragmentation of various affiliate networks and caused a ripple effect for the RaaS business model. This outcome may seem counter-intuitive; instead of reducing the number of Threat Actor groups, they multiply.

Threat Actors know that any link, no matter how faint, to a sanctioned entity or individual will likely rule them out of the running for a ransom payment. This means that any time an arrest is made or a new sanction put in place, the associated network typically splinters and affiliates re-brand in order to disassociate themselves from the black-listed group. We saw this with EvilCorp when they were sanctioned by the US Office of Foreign Assets Control (**OFAC**).

Open-source intelligence[11] suggests that since 2020, the number of active ransomware Threat Actor groups has increased dramatically year on year, from just 21 in February 2020, to a peak of 60 different groups in July 2023.[12] By active, we mean ransomware Threat Actor groups observed leaking data each year (although in reality, there are of course more groups that fall outside of this definition).

Number of Active Ransomware Threat Actor Groups



Source: Flashpoint[13]

Threat Actor groups and the RaaS model

RaaS is a cybercrime business model that can be likened to somewhat of a franchise arrangement. The ransomware group builds a brand, a reputation, and a corresponding ransomware code and then sells that to other gangs or 'affiliates' (i.e. franchisees) to enable them to carry out their own ransomware attacks. In return, the affiliate provides the ransomware group with either an upfront payment, subscription fees, a portion of the profits, or a combination of all three.

Practically speaking, when multiple different affiliates are using the same ransomware code and corresponding techniques, tactics and procedures, and identifying themselves as part of the same overarching group, this makes it very difficult (if not impossible) for forensic analytics to pinpoint one singular group / affiliate responsible for an incident. This question of attribution can become critical in the context of threat intelligence and sanctions analysis.

In reality, the RaaS model means that there are likely a number of actors involved in various elements of a ransomware attack.

This fragmentation can become difficult to navigate in the context of threat intelligence and incident response strategy.

Aside from attribution, the major upside of being familiar with the popular Threat Actor groups is that we have very detailed records of their past behaviours and are therefore able to make informed predictions about their likely next steps. This intelligence goes towards understanding a Threat Actor's motives, tactics, location, linguistics, connections with affiliate groups, the likelihood of data exfiltration, average ransom demands, and other relevant patterns of behaviour that can be a valuable to informing the victim organisations' decision making.

However, the constant introduction of new groups makes this increasingly difficult, as this limited track record means we are less able to reflect on a Threat Actor's past behaviour to predict how things may play out.

Negotiating blind

A professional body found themselves held to ransom by an unknown Threat Actor with zero track record. This actor had employed sophisticated techniques (so we knew this wasn't their first rodeo) however no one in the cyber threat intelligence industry had ever heard of them before – this made it very difficult to determine what kind of actor the organisation was dealing with and what to expect from them.

The organisation's data and backups were entirely locked up, and services had ground to a halt. The organisation determined they had little choice but to negotiate with the Threat Actor to secure the decryption key.

Ultimately, the absence of reliable threat intelligence meant the organisation was negotiating blind – most importantly, they had no sense of the likelihood that this Threat Actor would come good on their commitment to provide the decryption key in exchange for payment. The organisation undertook due diligence, technical and legal, to confirm the identity of the Threat Actor as best they could prior to payment.

Following payment, the Threat Actor proved their reliability and pulled through with the agreed deliverables. This Threat Actor later grew to be prominent and active in the cyber threat landscape, with a lengthy and consistent track record.

Spotlight: the prolific 'LockBit'

LockBit ransomware first appeared in September 2019. It has seen a number of variations, with LockBit2.0 appearing in 2021 and LockBit 3.0 in 2022. LockBit3.0 is reported to have similarities with BlackMatter and Alphv/BlackCat ransomware, and the margins between groups blur.

Today, LockBit is the most active cybercrime organisation globally. This gang employs the well-established RaaS model, and is known to encrypt files, steal data, conduct multilayered extortions, and threaten to publish the stolen data if payment is not made. Most importantly, if a settlement is not reached, the likelihood is that they will turn the threat of data publication into a reality by exposing stolen data on their Data Leak Site.[14]

Keeping it professional

LockBit operate much like a business and have their own 'code of conduct'. The LockBit ransomware operators provide malware and tools to individuals or organised crime groups (otherwise referred to as 'affiliates') to carry out the attacks, in exchange for a share in the profits. The group take their anomynity seriously - offering a reward to anyone who can reveal their identities.

LockBit are selective in their targeting, programming their offering in a way that cannot be used in attacks against Russia / CIS countries (Commonwealth of Independent States). This is likely a precautionary measure taken by the group to avoid any backlash from the Russian government and provide them with safe harbor from extradition.[15]

LockBit are a force to be reckoned with, and it's good for business. As more attacks accumulate on their Data Leak Site, so too does the recruitment of new affiliates to their RaaS business model.

Sanctions considerations

Before making a ransom payment, organisations must carefully consider the risk of breaching relevant sanctions and criminal laws. This includes taking reasonable precautions to ensure that proper checks and due diligence screenings are conducted prior to making payment.

Picking up on the above challenges regarding the nature of Threat Actors and the RaaS networks they operate in, it can be very difficult (again, if not impossible) to precisely identify who is on the other end of a ransom payment. This inability to confirm with certainty which individual(s) or entity sits behind the Threat Actor's façade, means there is always an inherent and unavoidable risk associated with making a ransom payment.

When undertaking reasonable precautions and due diligence, certain factors (such as the Tactics, Techniques and Procedures used by the Threat Actor, evidence of geographical links, IP addresses, linguistic cues) must be considered.

These factors can be helpful in informing whether there are connections to a sanctioned individual, region company or group, that may elevate the risk that payment will result in a breach of sanctions law.

Access linked to Iranian University IP address

A victim organisation was leaning towards paying a ransom demand, so engaged two independent threat intelligence vendors to undertake due diligence on their behalf.

One due diligence report cleared the payment, citing no apparent links with any sanctioned entity or individual, while the other identified a link between the Threat Actor and a university in Iran (a region subject to sanctions prohibitions) via an IP address. Although this specific university was not listed on the Department of Foreign Affairs and Trade's "Consolidated List", several Iranian universities and government officials are listed.

Despite being unable to definitively identity the Threat Actor as a designated individual or entity, the links to a government-owned Iranian university significantly increased the risk that payment could potentially constitute a breach of Australian sanctions laws, by way of making an asset directly or indirectly available to a sanctioned Iranian entity or individual.

As a result of this heightened risk, the organisation determined not to proceed with the ransom payment.

Key finding 3: **Decline in payment of ransom demands**

We've already discussed how the ransomware landscape has transformed via the increase in data extortion, the decline in encryption, and the evolution of Threat Actor groups. However, the main component of a ransomware attack is the payment considerations at the other end – in other words, how well Threat Actors can convert these attacks into a payout.

Taking a step back, there are several reasons why an organisation that has experienced a ransomware attack may be inclined to reach a settlement with a Threat Actor and (subject to legal and sanctions clearance) pay a ransom demand. Our sense is that all things being equal, Boards are driven by the question of 'what is the right thing to do' noting that the decision is within their control.

In our experience, the top reasons why victims pay ransoms include:

- if backups are not available and the decryption key is essential to unlock encrypted data and systems to mitigate business disruption;
- to confirm the scope of compromised data ahead of a data publication event and support targeted notifications to affected individuals;
- to prevent the publication and wider misuse of personal information about individuals;
- to avoid adverse publicity associated with incident details in the public domain and limit undue alarm and concern to stakeholders;
- to protect the dissemination of otherwise commercially sensitive or other protected information; and
- to stop Threat Actors from engaging in escalated activities including secondary extortion tactics against other businesses and individuals.

While these reasons are all pragmatic, and in some instances critical to resuming operations or figuring out what data was impacted, they do not take away from the inherent risk associated with doing a deal with a cyber-criminal. Clearly any payment of a ransom demand perpetuates and incentivises further activity.

Against all of this, there is a strong public sentiment that Threat Actors are inherently unreliable and therefore payment of a ransom cannot be relied upon as any sort of assurance that data won't be retained and misused at a later date.

The reality is that every Threat Actor is different; some are incredibly unreliable and have a high default rate (particularly years later), and others have a flawless track record of keeping their end of the deal. Overall, any decision should be based on informed advice from threat intelligence experts and weighed up against data risk and available evidence.

In our experience, Boards and authorised decision makers do not take this decision lightly – there is often 'remorse' either way.

Why organisations decide to pay

A professional services firm suffered a major attack impacting multiple servers – several servers were encrypted, and others showed signs of 'data staging' indicating that files had likely been exfiltrated.

The organisation decided to engage with the Threat Actor to validate whether data had been exfiltrated. In the course of this engagement process, the Threat Actor provided a list of files representing over 100 gigabytes of data that it claimed to have taken – this list detailed a range of sensitive materials including client data and internal commercial financial information. The Threat Actor subsequently validated that it was in fact in possession of that data.

After thoroughly considering its legal obligations (including the legality of ransom payment and relevant sanctions regimes), as well as strategic commercial considerations and risk of dark web publication, the organisation concluded that paying the ransom was **necessary to prevent the disclosure of sensitive information**. This was notwithstanding that majority of the data at risk of disclosure pertained to corporate clients, as opposed to individuals' data, and risked exposing quite sensitive commercially protected information.

The organisation reached a settlement with the Threat Actor, making a ransom payment in exchange for the return of data, provision of a decryption key, and a commitment not to publish or on sell any exfiltrated data. The Threat Actor provided the agreed deliverables, and to this date, the data has not been published.

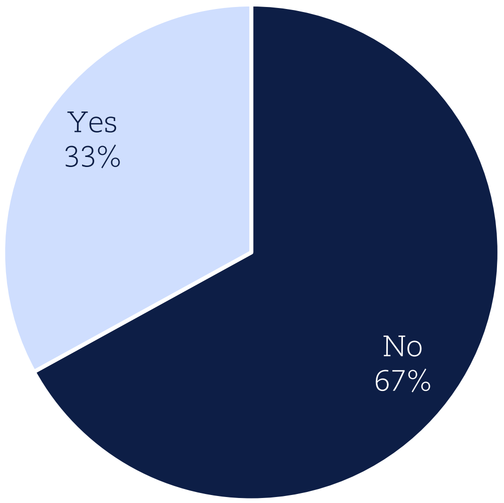
During the Analysis Period, we saw a substantial decrease in the frequency of ransom payments.

While we've seen a return of big game hunting tactics with a focus on targeting larger enterprises for maximum payments, Threat Actors are often indiscriminate and target an array of organisations (or at least, target vulnerable end points to see what they can find). This means that while large corporates have recently not paid, the same can't be said for smaller organisations or Managed Service Providers (**MSP**) that have become a ripe target for Threat Actor groups.

Coveware, reflecting on their combined aggregated ransomware case data ransom payment trends over the past four years, observed that the willingness of victims to pay ransom demands **dropped from 85% in Q1 2019 to 37% in Q4 2022.**

Within the Analysis Period, Coveware reported an **annual payment rate of 41%**. Our own statistics show a similar rate of payment – **33%** of ransomware Incidents during the Analysis Period.

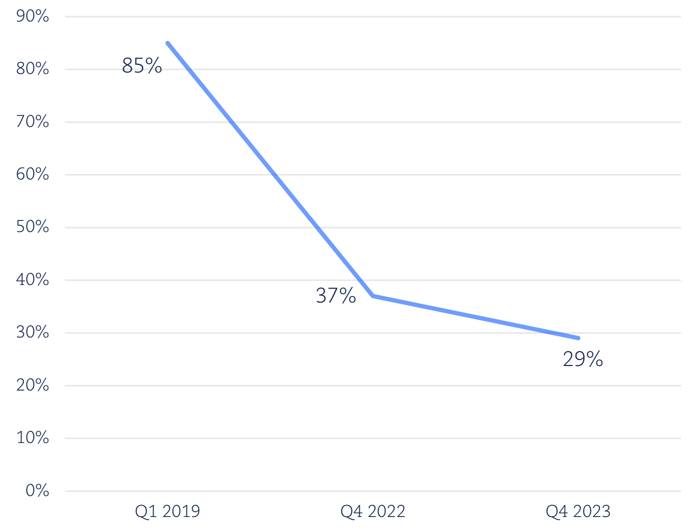
Ransom demands paid during Analysis Period



The downward trend in ransomware payments has continued through 2023.

Coveware note that in the first half of 2023, the percentage of ransomware attacks resulting in victim payments hit a **record low of 34%**. By the end of 2023, the proportion of victim organisations that opted to pay ransoms had dropped to a **record low 29%**.

Trend in Payment of Ransom Demands



Source: Coveware[17]

In our view, there are several reasons for this decline in ransom payments, notably:

- greater investment in cyber resilience and readiness programs, meaning organisations are better equipped to respond to ransomware attacks and less frequently need to purchase a decryption key from the Threat Actor;
- heightened attention and scrutiny from law enforcement and government;
- introduction of broader sanctions and the socio-economic impact of the Russia-Ukraine war;
- strategic shift by law enforcement agencies to focus on victim assistance (e.g. the FBI's takedown of Hive ransomware group in the second quarter of 2022 and the takedown of BlackCat servers at the end of 2023 as examples of where Australia has benefitted from AFP involvement in disrupting RaaS groups);
- a strong push from the Australian government and industry against the payment of ransoms;[16] and
- increased corporate willingness to make a stand against payment and allow data publication events.

Of course, at the same time, there has been a sharp increase in privacy claims, class actions and regulatory investigations following ransomware events. It remains to be seen what further law reform and policy initiatives will do to influence this downward rate of payment.

One thing appears certain, we are heading in the right direction

Surge in 'big game hunting' despite record low ransom payment rates

While the downward trend of ransom payments is encouraging, the flipside is the further evolution of attack and extortion tactics by Threat Actors. Namely, while the frequency of ransom payments has gone down, the average quantum of ransom demands (particularly those targeting larger organisations) has increased.

Naturally, the trend of decreased frequency of ransom payments correlates with higher demand quantum, namely if Threat Actors aren't getting their pay outs as often, they will charge more.

Towards the end of 2023, Coveware noted that globally, victim organisation' were paying substantially higher ransom amounts than in the first half of 2023.

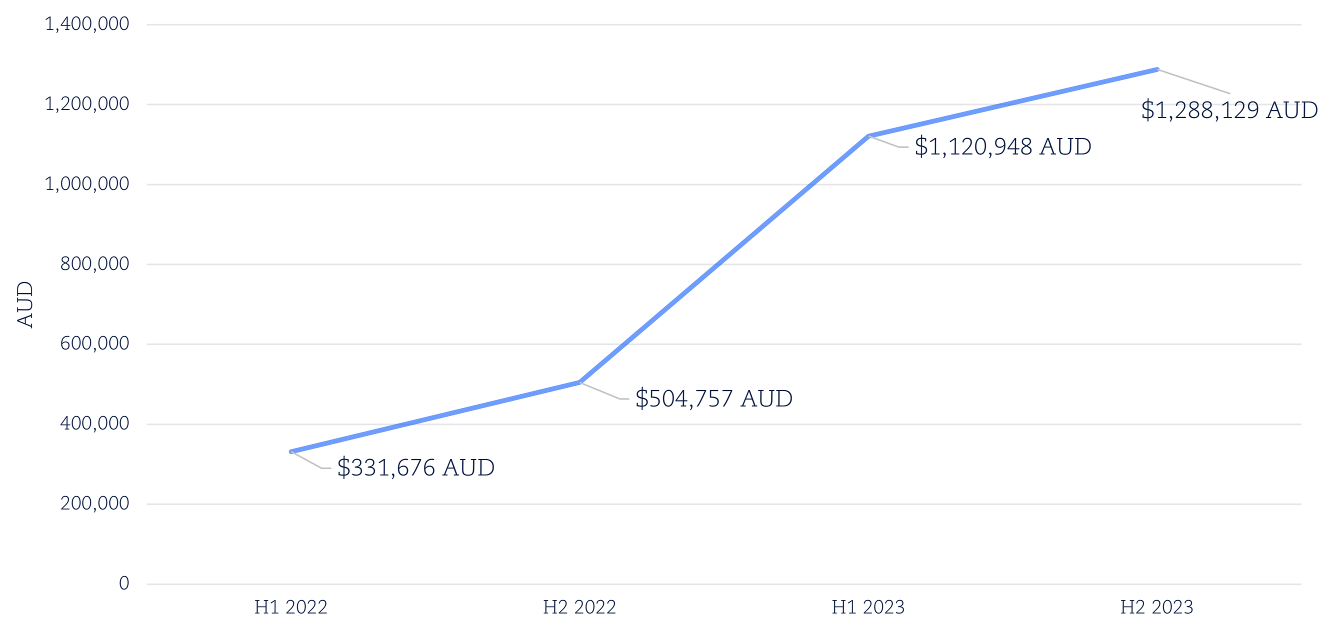
As an example, the Threat Actor group CloP's exploit of an international file sharing company in May 2023 led to a spike in Coveware's global average ransom quantum up to $740,144 USD ($1,123,982 AUD).

Coveware observed a further increase in both average and median ransom payments in Q3 2023, with the average ransom payment rising to $850,700 USD ($1,292,638 AUD), and the median ransom payment ticked up to $200,000 USD ($303,900 AUD).

While we're seeing a positive decrease in the rate of ransom payments in Australia, globally the quantum of ransomware demands are increasing, with Chainanalysis reporting that ransomware payments in 2023 surpassed $1.1 billion USD ($1.68 billion AUD).

While we are heading in right direction to defend against ransomware attacks and resist the payment of ransoms (in Australia), we are not out of the woods yet. Threat Actor's are fully funded and ready to go. The significant funds being made available to Threat Actors globally will become our problem in the near future.

Quantum of Ransom Demands – Yearly Average

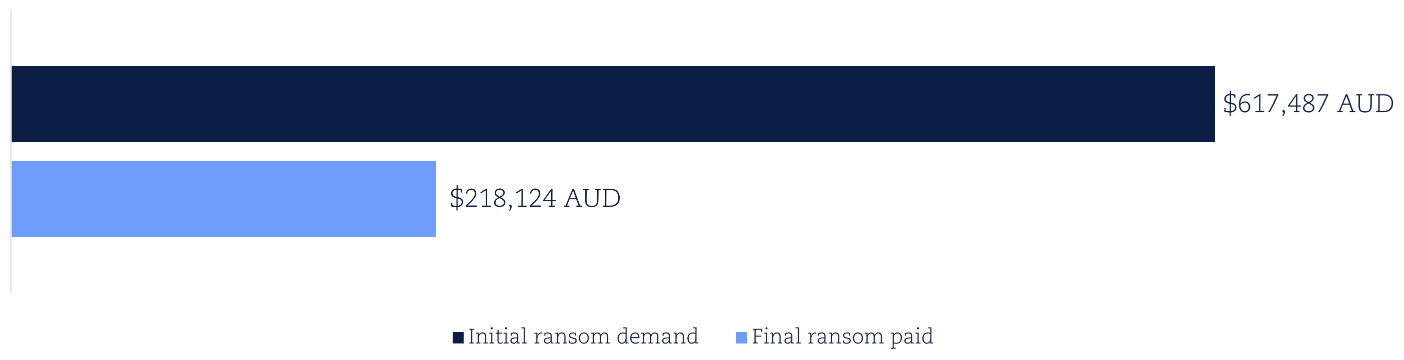


Source: Coveware

While we have seen an increase in the quantum of ransom demands (i.e. initial demands), our data indicates that victim organisations are successfully negotiating these demands down prior to reaching a settlement figure.

On average, following negotiations we see a decrease of approximately 65% from the average initial ransom demand made to the average final ransom amount paid

Average Ransom Demand vs Ransom Paid during Analysis Period



Negotiating for the sake of protecting sensitive health information

While we've seen a return of 'big game hunting' tactics that focus on targeting larger enterprise for maximum payments, the reality is that ransomware actors do not discriminate.

A small but influential healthcare entity experienced a ransomware incident in which high risk, sensitive health data was compromised. The Threat Actor demanded a ransom payment, and threatened to publish the data online if the ransom was not paid.

Considering the type of information impacted and vulnerable group of individuals that it related to, the organisation ultimately decided to make the ransom payment to avoid publication. The organisation determined that the harm to the individuals was too great of a risk to bare, in light of the incredibly sensitive nature of the data and profile of affected individuals to whom the data relates.

As a result of negotiations, the Threat Actor reduced the ransom amount from the initial demand. Following payment, the Threat Actor provided the agreed deliverables, and to date there is no evidence that the organisation's data has been on-sold or published by the Threat Actor.

Other key findings: **Root cause analysis**

It's only natural that when a cyber incident occurs, stakeholders want answers to 'how did this happen?' and 'what do we need to do to ensure this doesn't happen again?'.

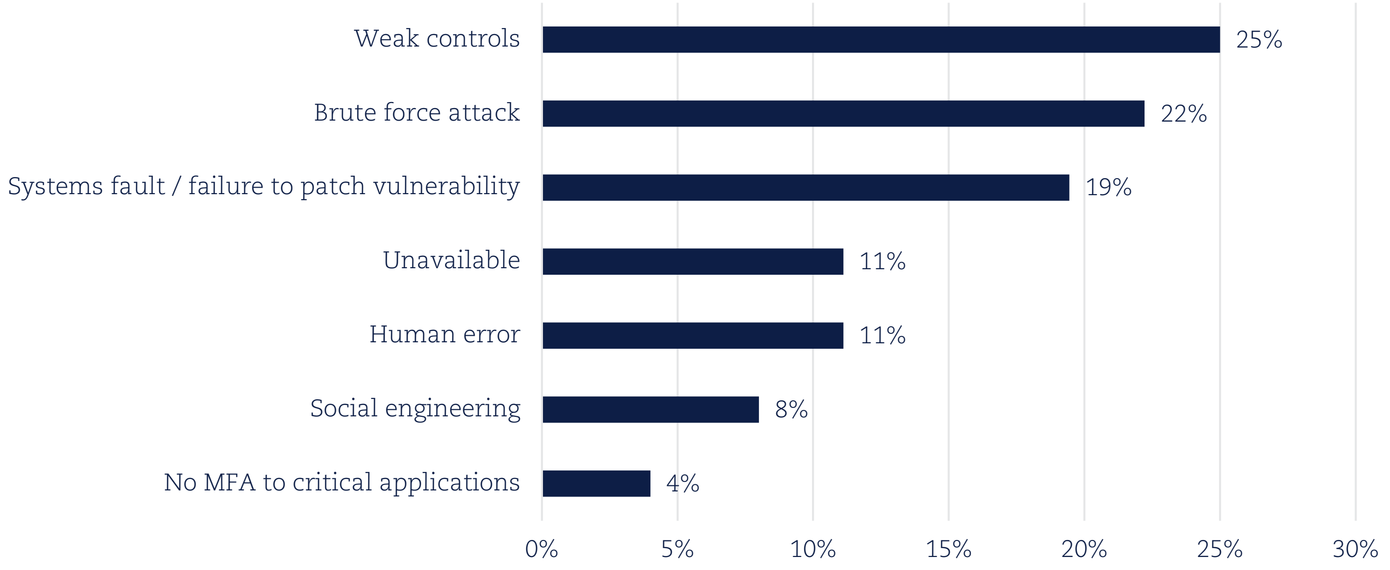
It is for this reason that organisations regularly engage external forensic investigators dual qualified with security expertise to undertake root cause analyses.

During the Analysis Period, our data indicates that the leading cause of the Incidents involving ransomware 'weak controls'. For the purpose of our analysis, 'weak controls' was defined as a flaw in the design or operation of a procedure or protocol.

Specifically, the majority of the Incidents in this category were attributable to the compromise of a Remote Desktop Protocol (**RDP**) port, involving a Threat Actor exploiting a legitimate remote access feature to appear as a legitimate user and gain system access and control (as opposed to relying on human error alone or a system vulnerability).

As this involves the use of a genuine control feature, anomalous activity can be very difficult to detect. In our experience, the popularity in RDP compromise as a main attack vector is likely opportunistic for Threat Actors, becoming an easy target with the rise of work-from-home arrangements.

Root Cause of Ransomware Incidents during Analysis Period



Following closely were:

- **Brute force attacks (22%);**
  A brute force attack uses trial and error to crack passwords, login credentials, and encryption keys – a simple yet reliable and clearly effective method of gaining unauthorised access. While the widespread adoption of multi-factor authentication has helped to mitigate brute force attacks to some degree, in our experience, multi-factor authentication (**MFA**) fatigue has crept in, allowing Threat Actors to bypass these controls.

  To reduce these risks, organisations are enforcing strict patching protocols, deploying advanced threat detection technology, improving employees' security awareness and monitoring the dark web for any data leaks or stolen credentials.

- **Systems vulnerabilities (19%); and**
  Systems vulnerability/failure to patch vulnerability describes those incidents where a Threat Actor has exploited an unpatched software vulnerability (such as an API vulnerability). Unpatched software refers to applications or systems that contain known vulnerabilities that have not yet been addressed through the implementation of updates or patches.

  Threat Actors are often aware of vulnerabilities before patches are released, meaning it is crucial to keep systems updated and patched using a clear patch management strategy.

- **Unknown (11%).**
  While there are mitigants available for majority of these attack vectors, the fear lies in the 'unknown' category – that is, incidents in which the forensic root cause analysis has been inconclusive.

  It is common for Threat Actors to undertake anti-forensic techniques, aimed at reducing (or entirely eliminating) the presence of forensic evidence, or in other words, to cover their tracks and prevent a conclusive investigation. This inherently makes the investigation, as well as containment and remediation phases more challenging and presents the risk that the attack vector remains open for future attacks.

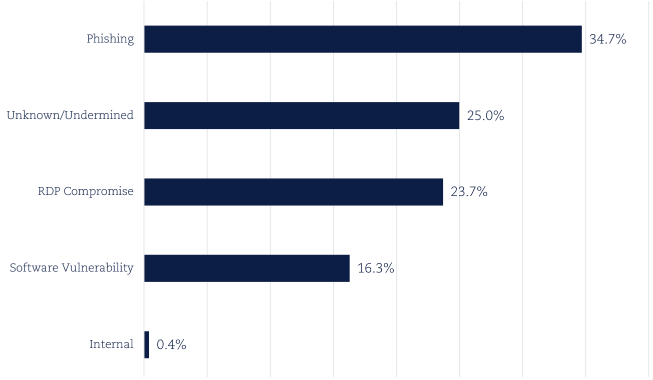
  It also erodes the victim organisation's trust internally, and limits what the organisation can project externally about whether it is 'safe to do business with'. This can lead to loss of business, reputational damage, and business interruption losses.

Coveware's data on initial attack vectors

Coveware's data during the Analysis Period similarly noted a high percentage of RDP compromises, software vulnerability and unknown/undetermined as an initial attack vector.

Notably, of the cases Coveware observed, phishing was listed as the most common initial attack vector. Cross-referenced with our categorisation, human error and social engineering rates tell a similar story. Phishing is a form of social engineering, whereby Threat Actors deceive individuals into revealing sensitive information or click a unsecure link, installing malware (such as ransomware). By nature, phishing relies on human error and misjudgement – clicking on a link you shouldn't. Coveware's data on the prevalence of phishing as an initial attack vector is therefore to be expected and aligns with our statistics on social engineering and human error.

Initial Attack Vector



Source: Coveware

The most popular extortion tactics

As we've touched on already, extortion tactics are central to the ransomware business model as they are commonly relied upon to pressure victim organisations into paying a ransom demand.

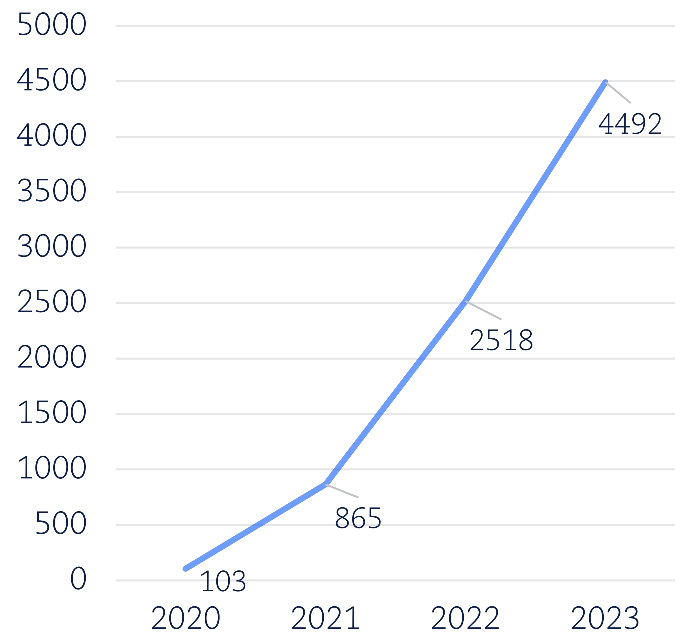
It won't come as a shock that the publication of data online was the most prevalent extortion tactic deployed by Threat Actors, followed closely by name staging on a Data Leak Site. In reality, these extortion tactics often go hand in hand, with the name staging being a precursor and imposing a degree of pressure on a victim organisation without throwing away too much leverage.

Number of entities published to ransomware group data leak sites

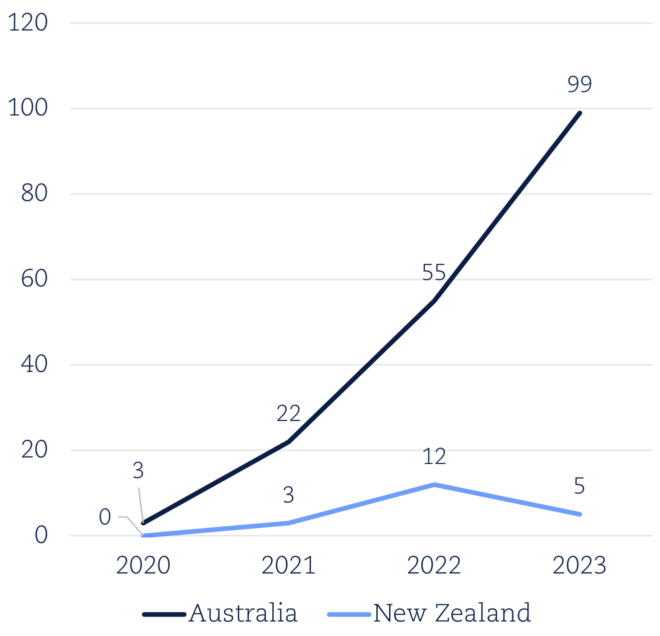
The number of Data Leak Site publications are increasing year on year both globally, and in Australia. The downward trend in number of New Zealand entities published on Data Leak Sites in 2023 is something that is unique to this market, as it is not something we have observed globally.

Our data shows that as the number of organisations paying ransom payments is decreasing, the number of publication events on Data Leak Sites are increasing. This reflects the final phase of the ransomware business model, whereby if an organisation refuses to pay the ransom demand, the Threat Actor will publish exfiltrated data online.

Entities Published to Ransomware Group Data Leak Sites - Global



Entities Published to Ransomware Group Data Leak Sites - AUS/ NZ

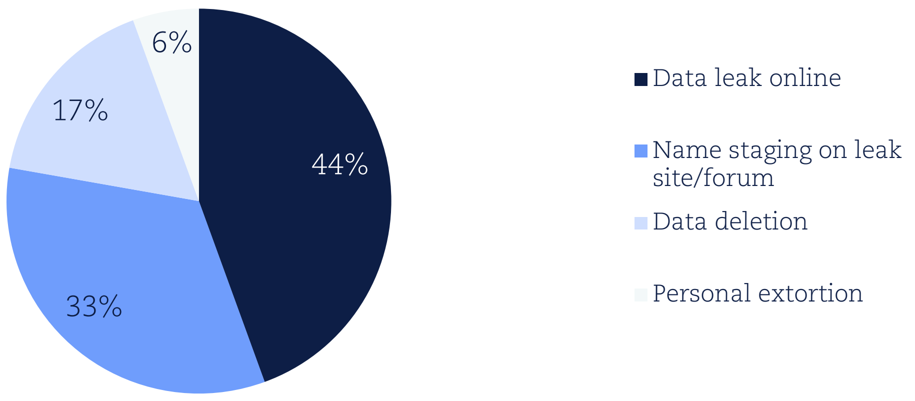


Source: Flashpoint

In our experience, this combined strategy is popular with Threat Actors for a number of reasons, including:

- name staging can be very effective at forcing a victim organisation to engage with the Threat Actor, with the goal of having their name removed from the Data Leak Site – this is particularly the case in circumstances where details of the incident are not otherwise in the public domain and the organisation is sensitive to media attention;
- drip feeding batches of sensitive data can spook a client into making a payment to avoid further reputational harm and to protect sensitive commercial or client data; and
- it is part of their business model to follow through on the threat of data disclosure – if they didn't follow through, the threat wouldn't hold the same weight and victims would be less inclined to pay for the suppression of stolen data.

Extortion Tactics Deployed



Extortion tactics of a persistent and volatile Threat Actor

What began as a single ransomware incident quickly developed into a BEC, direct contact with clients and staff, and a broader systems compromise.

The initial ransomware incident involved the exfiltration of data and encryption of all workstations, meaning employees were prevented from completing their duties. The organisation was able to recover from backups (meaning they did not need to purchase the decryption key from the Threat Actor) and ultimately took the position that they would not engage with the Threat Actor or pay the ransom demand.

Aggravated by the lack of engagement, the Threat Actor used stolen credentials to access various employee mailboxes and distribute confidential client documentation to ~4,000 staff and clients via email. The email was highly inflammatory and personal, stating that the organisation is not trustworthy and does not care about its clients, and threatening to leak private and confidential data if a ransom was not paid.

When the organisation did not respond, the Threat Actor subsequently launched the third and final component of its attack, compromising the organisation's key financial and practice management system, exfiltrating thousands of files, and deleting ~330,000 critical files from the platform.

The volatile and repeated attacks made crisis management and communications incredibly challenging, causing significant distress to clients and staff. A ransom was not paid and the victim organisation stood up to the Threat Actor's behaviour.

Deep Dive Topic 2: Business Email Compromise

Business Email Compromise

What is a business email compromise?

Business email compromise (or **BEC** for short) is a very common cyber incident type that continues to be lucrative for cyber criminals. Given their frequency, it can be equated to the modern-day cyber 'slip and fall'.

In simple terms, a BEC incident is a mailbox breach – a targeted attack where Threat Actors gain unauthorised access to a user's mailbox by logging into their account through deception, often bypassing security controls to do so.

BEC incidents almost always require the mailbox user to 'click on a link', surrender their credentials to open a document, or approve MFA tokens to provide the Threat Actor with unauthorised access to the account (called 'social engineering'). Hence, human error is typically the predominate primary cause of loss.

Threat Actors can also obtain usernames and passwords from other companies' data breaches where corporate usernames and passwords are exposed (called 'credential stuffing'). This is why it is important not to use the same or similar usernames and passwords across multiple online accounts, to use a password manager to store long complex passwords, and to have MFA in place for as many online services as possible.

Like all cyber-crime, BEC Threat Actors are financially motivated with the primary objective commonly being to perpetrate funds transfer fraud (**FTF**). BEC Threat Actors will often spend weeks or months in a compromised mailbox to learn how the unsuspecting user communicates with others, their role within the organisation, and communications cadence, before jumping in and taking over email traffic to commit FTF.

Sometimes, fake email addresses are set up by Threat Actors, and similar domains are registered to mimic the organisation that is about to be defrauded. For example, the letter "i" is replaced with "1". This allows the Threat Actor to keep communicating with parties outside of the compromised mailbox under the guise of an almost identical address, well after the mailbox has been secured.

Once inside a mailbox, Threat Actors commit FTF by manipulating invoice payment details or emailing parties to say that their bank account details have changed – thereafter providing the details of the Threat Actor's bank account in place of the organisation's legitimate bank account. These bank accounts are mule accounts set up by organised crime syndicates within Australia.

Often, neither the mailbox user, nor those with whom they communicate, are aware of the incident until something goes wrong or the incident is otherwise uncovered. Typically, this is when a supplier calls and queries unpaid invoices, which have already been paid by the compromised victim organisation, or suspicious mailbox activity is identified (such as out of country logins, or deletion of emails).

Finally, once a Threat Actor has what they need out of one mailbox, they will commonly use that mailbox to perpetuate a further phishing campaign; for example, send thousands of phishing emails to the user's internal and external contacts, in the hope that someone clicks on the link and surrenders their credentials – thereby providing the Threat Actor with further unsuspecting victims to continue the vicious cycle.

In years gone by, mailbox technology has been abused to send more nefarious attachments such as during the 'Emotet' crisis in 2019 – where users right across the world were sent attachments which would auto-execute upon receipt, triggering the mass harvesting of email content and mal-spam being further distributed.

What are the hallmarks of a BEC?

A BEC is likely to have occurred where there has been evidence of unauthorised activity in a mailbox. For example, mailbox forwarding rules being set up, logins from strange IP addresses, activity outside of work hours and / or unexpected password resets and MFA login prompts.

For many organisations, the first time they become aware of this is when a third party receives a request from a supplier to update payment details for outstanding invoices. Given how infrequently companies change bank accounts – this should be treated as highly suspicious behaviour unless properly verified over the phone (not by responding to the email sender aka the Threat Actor).

What is FTF?

As above, FTF describes the end stage of the BEC attack lifecycle in which a Threat Actor poses as the legitimate mailbox user, and sends a fabricated invoice or email requesting payment via a fraudulent bank account.

Commonly, the recipient has a pre-existing relationship with the legitimate mailbox user, and the Threat Actor will leverage the same language, syntax and tone that the mailbox user would ordinarily use, to legitimise their FTF request.

Mailboxes belonging to the C-suite or individuals that regularly deal with funds (such as members of a finance team or other financial controllers) are key targets for FTF. Once a Threat Actor gains access to these accounts, their position of authority is abused to bolster the legitimacy of any FTF request issued.

We also see professional service providers (such as law firms, accountancy firms) increasingly fall victim to this type of attack, as requests for bank account changes are typically treated with less suspicion by clients and counterparties. This is particularly the case where vendors are onboarded for the first time, or in the context of large one-off payments.

Further, professional service providers often deal with large sums and a higher frequency of payments, rendering the chance of successful FTF much higher.

It is important to remember that while not every BEC involves a successful FTF, every successful FTF involves a BEC which needs to be investigated by the parties involved, to confirm whose mailbox has been breached, what invoices are at risk of payment redirection, and what personal information has otherwise been accessed by the Threat Actor.

What are the non-financial implications of BEC incidents?

Depending on the method of access by the Threat Actor and contents of the mailbox itself, it is typical that personal information contained in the mailbox will be accessed by the Threat Actor as part of their overall activities.

In some cases, entire mailboxes can be downloaded and retained by the Threat Actor even after the account is secured. This is a key forensic question that needs to be determined and is often dependent on whether logging is available.

We have seen BEC incidents act as the precursor to, or an additional activity alongside, much more serious incidents such as ransomware attacks. Occasionally we have observed the targeted misuse of mailbox contents, such as data theft extortion and misuse of data against individuals emanating from mailbox breaches.

Depending on the industry, such as the property / conveyancing industry, the invoice fraud may hold up the settlement of a property transfer, leading to financial penalties for delayed settlement.

In many cases, purchasers cannot complete the transaction while the proceeds of the FTF are traced and recovered, or otherwise paid twice by the purchaser. In commercial transactions, the loss of funds may jeopardise a commercial transaction, or otherwise cause friction between otherwise friendly counterparties and suppliers.

Houston, we have a BEC problem

While ransomware incidents get the most airtime – being plastered daily across national headlines, grabbing the attention of political agendas, and frequently on the agenda for discussion at board meetings – BECs (including both pure BEC incidents and FTF) are in fact much more frequent.

Depending on the size of the FTF loss, the sums can be significant, often far outweighing any ransom demand paid to cyber criminals. For example, we have seen FTF losses exceed over $10 million AUD (in one incident alone) which is far greater than most average ransom demands in the current market.

Compared with ransomware, FTF losses are arguably a much bigger financial loss risk to the Australian economy than ransomware will ever be, and is something that warrants closer attention.

FTF is an exponentially increasing issue as organisations rely on email to distribute invoices and to provide payment instructions daily. Our data collected within the Analysis Period confirms that BECs are the number one incident type, accounting for a 44% share of all incident types.

Moving beyond our data, the ACSC and Australian Signals Directorate (**ASD**) reported BEC and FTF as the top two most common types of cybercrime experienced by Australian organisations in 2022-23, reporting $80 million AUD in combined losses for year.[18]

We estimate conservatively that this represents only 15% of reported losses in Australia (our best guess is that about $500 million AUD is paid out of the economy annually through FTF).

Total worldwide losses are likely to be closer to over $2.7 billion USD annually ($4.1 billion AUD annually).[19] On the other hand, it is estimated that the payment of ransom demands amounts to $457 million USD annually ($694 million AUD). [20] Chainanalysis reported a spike in 2023 to $1.1 billion USD ($1.68 billion AUD) in ransom payments globally - the highest ever recorded. This spike correlates with the increase in average quantum of ransom demands globally in 2023 and the return of big game hunting, as discussed at page 28.

The best data we have in Australia is from the ACCC report,[21] which suggests a combined $224.9 million AUD in payment redirection losses. This is comprised of:

- individual reports made to Scamwatch ($24.8 million AUD);
- ReportCyber ($147 million AUD); and
- the Australian Financial Crimes Exchange ($53 million AUD) in 2022.[22]

Of these, there were 74,573 phishing scams reported resulting in $24.6 million AUD worth of losses, a 469% increase from 2021.[23]

Other data from the National Anti-Scam Centre's (**NASC**) 'Scamwatch' report noted 99,736 phishing scams reported in 2023.[24]

It is unclear how many BEC and FTF incidents are not reported annually, but whatever the true financial loss, the number of BEC and FTF losses and their frequency of occurrence in Australia is very likely higher than the reporting indicates.

What do our stats tell us?

Leading up to 2020, when MFA was more frequently utilised and staff phishing training and call back procedures became a cornerstone requirement for organisations, we expected to see the end of BEC incidents. However, with MFA fatigue creeping in, BECs have managed to maintain their pole position as a staple incident type.

From our data, BEC incidents have increased in frequency, which presents an enduring FTF risk exposure. The average FTF amount identified in the Analysis Period was $135,000 AUD; a sizeable sum and significantly higher than the $39,000 AUD average reported by the ASD.[25]

Based on data relating to FTFs captured during the Analysis Period:

- Only 17% of FTF incidents achieved a complete recovery (characterised as 100% of funds fully recovered) from the involved banks.
- In 78% of FTF incidents, no funds were able to be recovered with funds making their way into Threat Actor's pockets.
- Following a victim organisation's efforts to recover the misdirected funds, 5% obtained a partial recovery.
- Of the organisations that were able to recover the partial or entire FTF amount, 74% of those organisations recovered up to $50,000 AUD (remembering the average loss amount is $135,000 AUD).

The time to recover funds is a lengthy process and is not always guaranteed. As clear from our data, the prospects of recovering funds are slim. Attempts at recovery can take banks between 3 to 6 months before reaching an outcome, even where there is partial or whole recovery.

Our key findings follow.

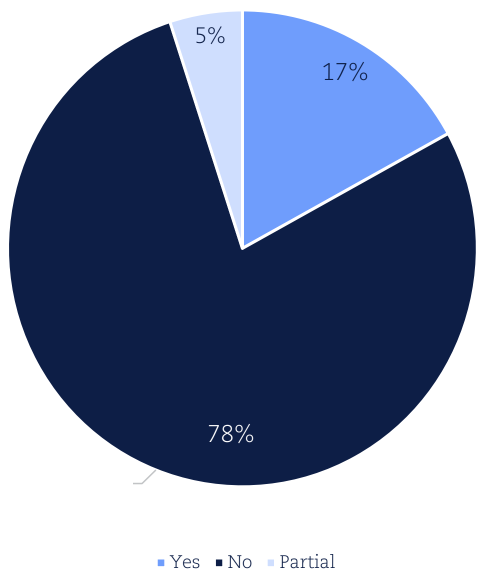
Spotlight: **FTF** statistics for the analysis period

Minimum FTF amount: $6,000 AUD

Maximum FTF amount: $735,000 AUD

Average FTF amount: $135,000 AUD

Success of recovery?



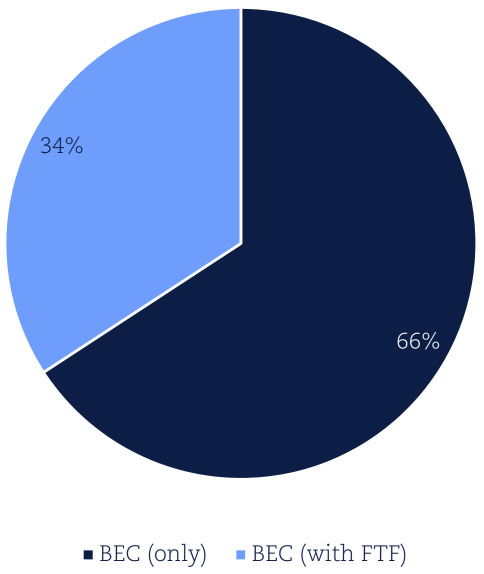
Key finding 1: **BEC and FTF on the rise**

BECs continue to be the favoured method of attack for Threat Actors. We have observed BECs and FTF continue to hold the number one incident type year after year, accounting for almost half of all Incidents (at 44%) during the Analysis Period.

This is demonstrated below, where both BEC and ransomware incidents combined make up a total 81% during the Analysis Period.

FTF was seen in 34% of all BECs, highlighting the prevalence of funds loss associated with BEC incidents.

Positively, FTF did not take place the remaining 66% of the time – highlighting that Threat Actors are not always successful in their objectives. This is largely due to enhanced detection, eviction and FTF prevention methods, such as telephone call back procedures being implemented.



Data misuse to commit FTF – 'Sign' of the times

An organisation experienced a sophisticated BEC incident involving FTF, resulting in the fraudulent misdirection of over $1.8 million USD. The Threat Actor gained access to the financial controller's mailbox and fabricated an acquisition process, complete with Board meeting minutes, CEO and director's signatures, a fake email trail between the financial controller and the CEO, and corresponding invoices.

The Threat Actor used these materials to circumvent the organisations usual approval processes. The accounts payable team executed the fraudulent instructions in good faith, and based on the belief that the prior emails and supporting documentation (including physical signatures) were legitimate.

By the time the organisation identified the FTF, the funds had travelled to a Malaysian bank account, at which point the account was frozen and remaining funds seized. As a result of the delay between transferring the funds and identifying the fraud, over $350,000 USD had already been withdrawn and considered unrecoverable. Following almost 18 months of correspondence with Interpol and local law enforcement, engagement with the corresponding banks, and eventually litigation, a portion of the remaining funds were returned to the organisation.

Industry focus: Property transaction vulnerability

Many property transactions are managed by small conveyancing businesses that lack technical support, cyber awareness, and funding to implement strong protective measures against cybercriminals.

On the purchaser's side, many individuals may only be involved in one or two property transactions in their lifetime. This means they are often unaware of the risks and standard call back procedures that should be undertaken to ensure the secure transfer of funds to real estate agents and conveyancers for deposits.

Often, the process of buying and selling a property can be very confusing and complicated for a purchaser, especially a first home buyer, with multiple parties, steps and procedures to follow. This, combined with an inherent trust in the service provider make it much easier for FTF to be committed. The bottom line is, ***"the value of houses has gone up, and there is a lot of cash flowing through the real estate sector,"***[26] – this makes the real estate market a particularly prime target.

Oh no, where's my deposit gone?

A purchaser was nearing their settlement date and received an email from their conveyancer, requesting that they transfer their deposit urgently and providing payment details for the transaction. Days later, the purchaser received another email from the conveyancer regarding the upcoming settlement and details on making payment.

It was later discovered that an unauthorised third party had gained access to the conveyancer's mailbox several months prior, quietly reviewing the conveyancer's protocols, changing forwarding 'rules', and isolating and redirecting emails sent by the legitimate conveyancer. This enabled the Threat Actor to commit FTF for an extended period without being detected.

A forensic investigation verified that the Threat Actor had compromised the conveyancer's mailbox, meaning that the conveyancer's cyber insurance policy was triggered and provided cover for the monetary value of the lost deposit.

However, by that time, the purchaser lost the opportunity to purchase the property.

Key finding 2: **No organisation is immune from a BEC and FTF**

Whether you are a small business operator or a multi-million-dollar organisation, Threat Actors are on the hunt for easy wins. Our data highlights that Threat Actors do not discriminate when it comes to organisations targeted. Centring in on this issue, BECs impact a range of private, non-profit, government and publicly listed organisations across all industries – no organisation is immune.

Organisations of all sizes, though particularly SMEs should consider obtaining a cyber insurance policy to provide covere for FTF. Notwithstanding that SMEs are the second most impacted industry from BECs, in our experience, they often neglect the importance of obtaining cyber insurance for several reasons.

In practice, a cyber insurance policy may respond to the FTF incident and cover the value of the misdirected funds, resulting in money back in the organisation's pocket.

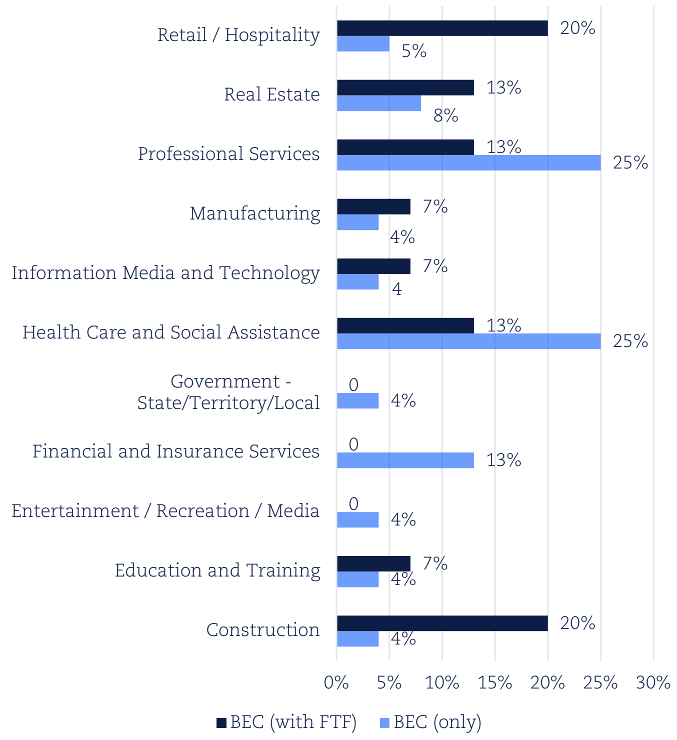
Key sectors impacted

During the Analysis Period, the professional services and healthcare service providers were the top two equally impacted sectors by BECs. This is likely reflective of the fact that the types of information present in mailboxes across these sectors is generally accepted as being highly sensitive in nature, and therefore a better target.

In the same vein, data recently published by the OAIC highlighted that in the first half of 2023, healthcare service providers represented the most impacted sector in the context of data breaches[27]; consistent with our data for both BECs and ransomware incidents. It is no surprise that healthcare service provides are data-rich targets for Threat Actors, given that they have high numbers of employees that have access to large volumes of sensitive personal information and health data.

In the context of BECs with an FTF element, the construction sector was reported as being the joint most impacted in 2023 during the Analysis Period, together with the retail / hospitality sector. In relation to the construction sector, this is likely a consequence of multiple high frequency progress payments being made to key suppliers over the lifetime of the contract.

Key sectors impacted



Key finding 3: **Social engineering and human error a leading cause of BEC incidents**

Root causes of BECs

Our data confirms that social engineering is over six times more likely to be the root cause of a BEC or FTF incident, over weak controls or a brute force attack.

Social engineering, including phishing attacks and quishing attacks are becoming increasingly sophisticated. For example, investigations are often uncovering that Threat Actors will implement a 'sit and watch' methodology while in a mailbox for a lengthy period of time.

In other words, once the Threat Actor gains unauthorised access to the mailbox, they will silently observe the legitimate mailbox owner's behaviour (including use of language and tone) and gather information from existing email communications, and then exploit those behaviours / background facts in order to mask the fraudulent communication as legitimate.

The second most common cause of BECs is represented in our data as 'unavailable'. 'Unavailable' is characterised by the root cause not being able to be identified, indicating that the organisation may not have completed a forensic investigation to determine the root cause of the incident, or that there was insufficient evidence available to conclusively determine how the Threat Actor got in.

This is often seen where an organisation does not have sufficient logging available in its Microsoft 365 environment, highlighting the importance of implementing logging beyond the default settings provided in Microsoft 365 to ensure that all relevant logs are collected.

The remaining portion of BECs were attributable to human error (such as an individual accepting an unauthorised MFA request), weak controls and brute force attacks.

Spotlight: **Root causes** of BECs

Multi-Factor Authentication bypass

- Ensure any requests for Microsoft 365 credentials are via a legitimate source, and only enter then details if you are sure the request is legitimate.

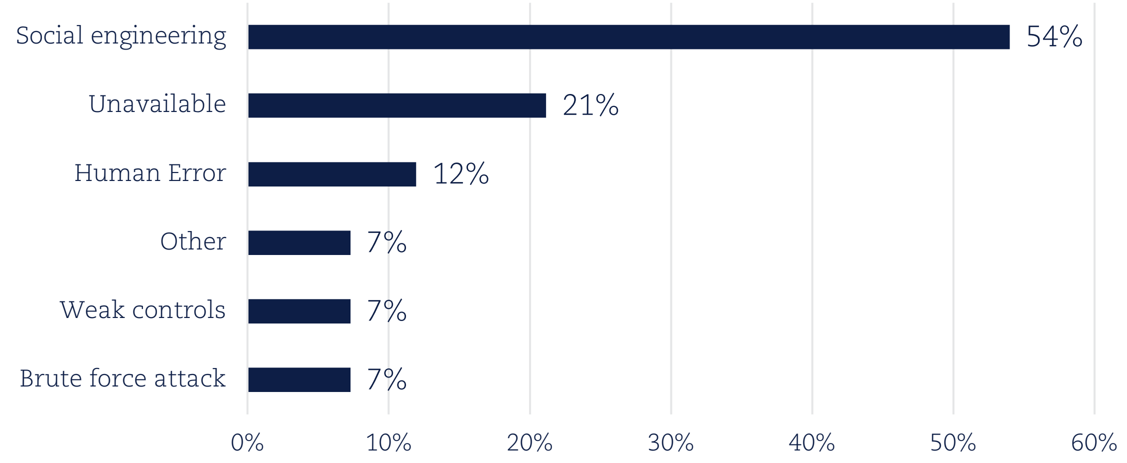
Human error (phishing)

- Remain vigilant for emails from people you haven't communicated with before, including those with attachments or asking you to click on a link.
- Check domain names to ensure that a Threat Actor isn't trying to trick you into legitimising their identify as someone else you are familiar with – it's all in the subtlety.
- Be mindful of urgent requests for payment – Threat Actors will aim to create a sense of urgency over their victims to action their request as soon as possible.

Call back procedure failure

- Whilst there is generally greater awareness for the need to confirm bank account details prior to transferring funds, we have seen an increasing uptick in organisations becoming complacent with this process.

Root Cause of BEC incidents during Analysis Period



Key risk factors

Our data highlights a number of factors that may increase the risk of falling victim to FTF, including:

- poor employee training leading to non-identification of scams and phishing attempts (for example, a user may click on a phishing link or open a suspicious attachment without recognising the danger);
- inadequate procedures in place to verify bank account details (such as call back verification procedures) before facilitating a transfer to a new bank account;
- the absence of MFA as an authentication step to stop unauthorised logins; and
- insufficient funds to invest in setting up more enhanced IT systems with access controls, audit logging and data loss prevention enabled.

New tactic – QR code phishing ("Quishing")

In an adaptation of the traditional phishing email, a Threat Actor (posing as an IT representative) requested the employee update their Microsoft Office 365 accounts by scanning a QR code embedded in the email - known as 'quishing'.

The scanned QR code led them to a phishing page via their mobile device, and therefore outside of the secure corporate IT infrastructure. The Threat Actor collected credentials and executed an account takeover, starting a chain reaction involving further phishing campaigns.

The QR code tactic was not picked up by company security software email filtering and seemed plausible to the employee, as many authenticator applications use QR codes for authentication. Threat Actors are evolving with the times, capitalising on both technological workarounds and MFA fatigue to bypass system and process controls.

Pre-approved account leads to major loss – Operation Dolos to the rescue

What began as a phishing email to an employee to steal credentials, quickly turned into a large loss event due to a combination of errors, including a systems' misconfiguration and human error.

An employee of a law firm accepted a phone call from someone purporting to be a case handler in the fraud department of a major Australian bank. The impersonator claimed to have identified various fraudulent transactions within the law firm's bank account, and managed to obtain a one-time banking token password from the employee, enabling them direct access to access the law firm's bank account.

A systems misconfiguration meant that the account hijacked by the Threat Actor was a 'pre-approved' account, meaning no further checks (i.e., authenticating the request to change details) were undertaken prior to funds being transferred.

As a result, several transactions amounting to approximately $6 million AUD were transferred to fraudulent bank accounts; two of these transactions were transferred to Australian bank accounts, one transaction was transferred to a Hong Kong bank account and one transaction was transferred to a US bank account.

The law firm identified the fraudulent transactions within the first 72 hours of initiating the transfers and immediately lodged a report with the ACSC and its bank. The AFP, working together with foreign jurisdictions and the law firm's bank, intercepted the misdirected funds and successfully recovered over 98% of the funds, returning these back to the law firm.

Australian Federal Police recovery efforts for FTF

The Operation Dolos Taskforce was created to provide a coordinated response to combat BEC including FTF within Australia. This taskforce consists of the Australian Federal Police (**AFP**) and all state and territory policing partners, the Australian Criminal Intelligence Commission, the ACSC, Australian Transaction Reports and Analysis Centre, and representatives of the Australian financial sector and international law enforcement.

Operation Dolos is dedicated to interrupting FTF Threat Actors and recovering funds. For increased chances of striking financial disruption, a FTF should be identified early enough – that is, within the first 72-hours following payment. This model is therefore reliant on a victim identifying and reporting the FTF as soon as possible.

We have seen that in incidents where FTF is identified and Operation Dolos engaged within the first 72-hours of the transaction taking place, the prospects of recovery are significantly higher, as compared to incidents that are acted upon outside the initial 72-hour window.

Key Takeaways

Organisations may be vulnerable even with the best controls in place	• Of course, organisations aren't perfect and as time goes on Threat Actors are becoming more adept to by-passing even the most sophisticated IT controls. • Ensuring regular patches and critical updates are implemented to your business email environment will ultimately enhance your security system. • It goes without saying that setting up solid MFA to access your mailbox will enhance security controls and limit unauthorised access attempts, especially in cases where credentials may have been compromised. Raising MFA awareness is key to ensuring a two-pronged approach to tighten accessibility to a mailbox. • Raising consumer awareness is key and organisations need to reinforce education amongst employees, including how to identify a phishing email. If you receive a 'phishy' looking email, attachment, docu-sign, gift card or QR code, do not click on it. It is best practice to report the email to your IT team to consider how to handle it. • Remain vigilant of bank account change requests and new contacts `requesting payment before processing a payment. Set up robust policies and procedures for employees to verify payment requests before initiating payment. • Organisations that permit 'bring your own device' must implement security requirements on the device to reduce the risk of unauthorised access via an employee's mailbox.
The future: working with banks to recover funds	• If you identify an unauthorised payment in your bank account, report it to your bank and the ACSC immediately. The earlier a FTF is identified, the greater chances your bank will have at intercepting the payment and recovering the funds. • Consider setting up MFA with your bank when initiating payments as an additional layer of protection to the pre-payment phase.

Deep Dive Topic 3: Third Party Breaches

Third Party Breaches

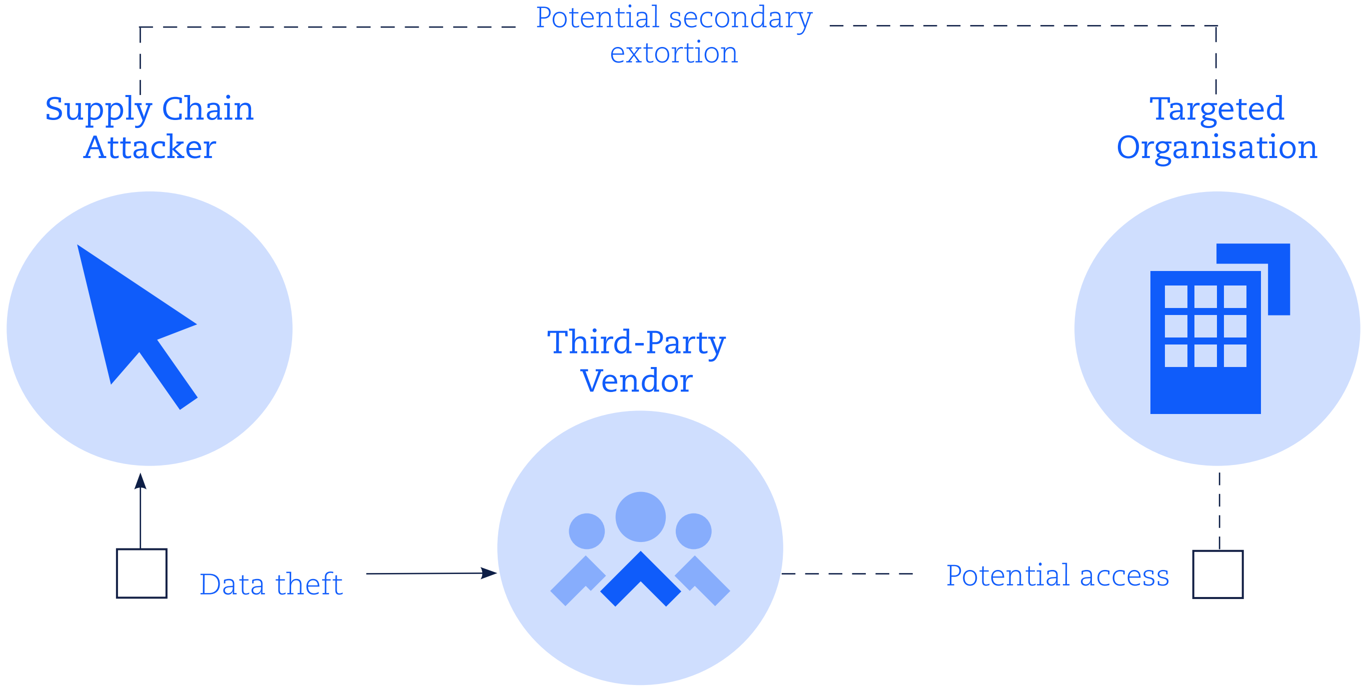
What is a third party breach?

Third party breaches refer to data breaches that arise from the system of a third party vendor such as a payroll service provider, product supplier or cloud-based storage provider.

Third party suppliers have increasingly become the target of cyber-attacks as they often store and have privileged network access to huge amounts of sensitive data belonging to many separate entities.

Depending on the type of provider, third party breaches have the potential to impose far-reaching ramifications across various industries. This is particularly relevant where the impacted organisation is a key service provider (such as an MSP) with access to the IT infrastructure of a large number of clients.

In recent times, the largest third party breaches have seen hundreds of clients impacted, and through them millions of individual's data compromised.



The beauty of this kind of attack for Threat Actors is that it allows them to broaden the scope of their attacks so that a single breach can be leveraged into multiple incidents impacting multiple victims. This strategy can also facilitate lateral movement into of some of the most well protected networks that would otherwise be beyond a Threat Actor's ability to directly compromise, and provides an opportunity for secondary extortion.

How big is the problem?

The rise in remote work post-COVID-19 has led to a significant uptick in the number of organisations relying on external vendors for software-as-a-service and web and data hosting.

For example, the Australian Bureau of Statistics reported a 16% increase in the number of Australian businesses that used Information and Communication Technologies such as software and cloud computing applications (from 69% in 2020, as compared to 85% in 2022).[28]

Amid the benefits brought by third party suppliers in streamlining supply chain management, reducing costs and leveraging expertise for enhanced security and operational efficiency, introducing an additional party to the supply chain inevitably increases an organisation's attack surface.

This exposes entities with even the most robust cybersecurity controls to the risk of a data breach through their supply chain – a breach of their data that is held by a third party.

This risk is most prominent in circumstances where an organisation inadequately manages the security controls of their third party vendors at the due diligence stage, and fails to implement ongoing monitoring practices to ensure its vendors follow and enforce proper security measures.

Threat Actors understand this and have shifted their focus to exploit a single upstream third party vendor to achieve maximum output from minimal effort.

While this attack type isn't new, the trend certainly saw an up-tick in 2023 compared to previous years. In Australia in particular, we have seen a number of large-scale incidents involving various HR-as-a-service providers, accountancy firms, legal service providers, e-discovery platform providers, and MSPs.

Key finding 1: **MSPs are often the weak link**

MSPs offer IT-related services to entities such as managing IT infrastructure and providing technical support and software. MSPs have become a preferred target as they often have remote access to the network of their customers.

Our data shows that **42.85%** of all third party data breaches across the Analysis Period stemmed from MSPs.

MSP breach

An IT MSP provided services to several customers operating across different industries, including healthcare, retail, and hospitality.

The MSP suffered a ransomware attack in which the Threat Actor utilised a public-facing exposure in the MSP's environment to gain access to a server that hosted data for various customers. The MSP had failed to properly segregate each customer's data, meaning that the Threat Actor was able to access multiple customers' data within the single server.

The Threat Actor exfiltrated data relating to multiple of the organisation's customers and proceeded to publish a 200 gigabyte dataset on its Data Leak Site. In the Threat Actor's post, it incorrectly attributed one customer as the sole owner of the published dataset, however the data was instead a combination of multiple customers' data (of the MSP).

One misattributed customer was named on the Data Leak Site, while another customer's data was contained in the published dataset.

These two customers (both of which were healthcare entities) agreed to a coordinated response to the incident – this involved a large data review and consequent notification campaign supported by the Department of Home Affairs' Cyber Security Response Coordination Unit.

The customers are now considering pursuing the MSP for its failure to protect their data.

Key finding 2: **Ransomware is the number one cause of third party breaches**

Ransomware stands out as the most common attack method for third party breaches i.e. **100%** of the third party Incidents identified from the Analysis Period originated from ransomware incidents or RaaS groups.

This is unsurprising as ransomware incidents provide an avenue for Threat Actors to monetise data threats efficiently.

This highlights the need for third party vendors – specifically MSPs with an interconnected network of clients – to bolster their cybersecurity resilience and response practices, and for organisations to understand their integration with third parties and potential risks stemming from outside their organisation[29].

File transfer applications are the perfect target

File transfer applications are often an attractive target for cyber-attacks, given they are regularly utilised as a central repository of large volumes of information.

In this particular case, a Threat Actor exploited a vulnerability in a file transfer program used by thousands of service providers across the globe. As a result, this singular incident impacted more than 60 million individuals.

While this incident did not directly impact Australian organisations, personal information relating to Australian individuals was housed within the application and breached as a result of the incident.

This is the perfect example of how the breach of a single vendor platform, if prominent enough, can have a phenomenally broad scope and impact.

Multiple payouts, one breach

A global tech firm provided file transfer services to hundreds of clients around the world, including healthcare providers, professional services firms, financial institutions and universities.

The file transfer application in question was in the process of being decommissioned, however there were a number of clients who were still actively using the application in advance of their transition to the new platform.

Before all clients were moved over to the new platform, a Threat Actor exploited a vulnerability that enabled them to access connected client networks and steal massive volumes of data.

Instead of approaching the tech firm for a single ransom payment, the Threat Actor approached each client individually and extorted them directly. This strategy – an example of 'secondary extortion' – lined the Threat Actor up for multiple payouts from a single breach.

The rising costs of third party breaches

The costs of third party breaches can vary depending on the type and size of the third party vendor and the nature of the breach.

As third party breaches generally affect more individuals than isolated ransomware and BEC incidents, IBM and the Ponemon Institute found that the average cost of a third party data breach is approximately $4.33 million USD compared to $3.86 million USD for general data breaches.[30]

Our general observation is that for the clients of an impacted third party service provider, the collective costs of dealing with a third party breach is significantly greater than dealing with an incident involving just the clients' own staff and customers' data.

This is usually because of the additional effort required to communicate with and support clients (that are typically operationally impacted by any system down time) as well as the costs of managing a large scale multi-party data breach.

There are usually also B2B liability costs associated with reimbursing affected clients for their consequential losses and liability arising from a joint investigation / and notification of the event.

Large-scale third party breach and a collective response

A professional services firm experienced a ransomware incident involving mass scale data exfiltration relating to multiple clients and other entities.

Given the broad scope of impact, a number of affected entities elected to progress a collective response. This approach created various efficiencies in the response process working closely with the victim organisation across the industry, to support with what was needed. For example, common knowledge regarding key incident developments was able to be shared effectively with the relevant parties to reduce response efforts.

It also meant that for the victim organisation, they could focus on their clients with little support as well as their technical response to the incident. For affected individuals, it was key to ensure consistent messaging around the incident details, the risk of harm to them, and the steps that they needed to take to prevent against data misuse.

This acts as a reminder that the industry has a responsibility to work together to achieve a collective outcome. This applies in respect of the breached entity, as well as the affected entities and individuals.

Protecting against third party breaches

Entities can mitigate the risks of third party breaches by adopting the following best practices:

Evaluate potential vendors: assess a vendor's security posture and data handling practices before onboarding them to ensure they have robust cybersecurity measures in place.

Align cybersecurity controls: ensure vendor's security policies, procedures and risk tolerances align and regularly assess for potential security vulnerabilities.

Risk mitigation in contractual agreements: integrate clauses with vendors that specify their obligations regarding security of jointly held data, notification obligations and indemnities for breach of security / privacy.

Enhance notification expectations: pre-determine expectations around the timely notification of joint breaches.

Mandate cyber insurance: ensure vendors hold cyber insurance (not just cyber liability insurance) to cover both the first party and third-party liability costs associated with a cyber breach.

Lead by example: industry leaders should support SMEs and medium sized businesses in the supply chain. We have seen a perfect example where large enterprises support suppliers with BEC and FTF mitigation, to prevent them (and their suppliers) being caught up in a web of scam email activity.

Deep Dive Topic 4: Other incident types

While ransomware, BECs and third party breaches account for 88% of Incidents in the Analysis Period, there are other incident types that occur. This section highlights the various types of cyber incidents that arise.

What other types of incidents do we deal with?

The 'other' types of incidents explored in this Guide include physical loss, software vulnerability, network access and website breach. These 'other' incidents make up 14% of all cyber incidents and span various 'at risk' industries including education, financial services, transport/logistics and healthcare.

Website breaches

'Website breaches' are defined as incidents that involve personal information or data accessed or exfiltrated from a database held on the website. Website breaches span equally over healthcare, government, retail and education and training and affect both the government and the private sector equally.

Software vulnerability – the need to have patch management in place

Our data over the Analysis Period highlights that software vulnerability incidents are evenly spread across several different industries – electricity, gas and waste services, real estate, and transport and logistics.

Threat Actors often exploit unpatched and misconfigured systems or take advantage of weak or re-used credentials to access systems and networks. In our experience, SME's, often overlook the requirement to patch software vulnerabilities, providing an easy access gateway for Threat Actors.

Guidance from the ACSC states that critical vulnerabilities in online services and internet-facing devices should ideally be patched within 48 hours, with regular vulnerabilities patched within 2 weeks to ensure best protective measures.[31]

Our data highlights that many incidents within the Analysis Period saw failure to patch critical vulnerabilities as the primary root cause of a cyber-attack.

Physical loss – someone's stolen my device!

Based on our data, physical loss incidents have predominantly affected small businesses. The data for stolen and lost assets illustrates the need for more secure ways to transmit data, and the need to encrypt physical hard-drives.

Other examples include stolen devices and misplaced assets in transit.

Cloud system breach

Our data revealed that network access incidents impacting cloud services was relatively frequent (typically impacting accounting software, and leaky online storage buckets).

Stolen laptop

A work device was stolen from an employee's car and handed up a criminal chain resulting in a Threat Actor gaining access to the laptop and mailboxes.

Fraudulent emails were then sent to a customer's bank, attempting to change fund recipient details.

Further unauthorised activity was detected on the employee's personal accounts, such as tampering with their myGov account and attempts to take out a bank loan.

In these circumstances, it is key to ensure that there are remote encryption capabilities on a work BYOD, so that the respective data held on the device can be remotely wiped as soon as it is reported stolen. Avoiding delay in reporting stolen devices is also crucial to intervene prior to fraudulent activity taking place.

Employee theft

Although not counted in our data across the Analysis Period, another key incident type we regularly respond to is employee theft of data.

This has seen a sharp uptick in the past 12 months, and is generally attributable to employee layoffs, M&A activity (and perceived or actual impending redundancies in a deteriorating economic environment) and employees looking to set up their own business.

Employee theft cases can be incredibly tricky to manage – both from a technical and HR perspective.

This is typically because the employee knows the systems incredibly well, and in turn, how to circumvent the monitoring. From a technical perspective, it can also be difficult to distinguish genuine activity from malicious activity in order to prove data has been taken dishonestly.

From an HR perspective, the way in which investigations are conducted and the conversations that are had with the employee (and other colleagues) present a uniquely complex set of circumstances and should be managed delicately.

Organisations should be alive to this and implement appropriate use standards, data loss prevention mechanisms, and be ready for a multi-faceted investigation crossing IT and employment relations teams.

Misattribution – a rising concern

The final incident type worth touching on (and again not collected in the Analysis Period) is the rise in misattribution. This typically occurs where a Threat Actor steals data of an organisation and misattributes the ownership to a third party – usually another organisation whose details are contained in the dataset but who does not control the systems which were breached.

Investigating and communicating with confidence through a misattribution event can be incredibly difficult, mainly because you are shadow boxing a Threat Actor's public claims alongside increased media interest. Victim organisations are often forced to prove a negative – establish that they weren't breached despite the contrary allegations.

Ensuring that organisations have a good handle on their supply chain and the data they hold is usually the starting point, as well as a strong crisis communication, and forensics capability including wide visibility over their network to confirm they are not under attack despite allegations to the contrary.

Scams and online fraud - Clyde & Co Pro bono

Over the years, scams against individuals have been on the rise and cleared many victims in their path. For individuals, the top four reported cybercrime types stayed the same as in 2021 to 2022, being identity fraud, online banking fraud, online shopping fraud and investment fraud. While we typically act for organisations, in certain circumstances we can and do assist individuals and not-for profits on a Pro Bono basis. Clyde & Co's National Pro Bono Program endeavours to provide employees with a practical way to contribute back to the community.

Giving legal assistance for free or at a substantially reduced fee to individuals, organisations, and non-for-profit organisations is a core part of doing our bit. Our firm's core values are to make our services accessible and signal to our clients that we value more than just the bottom line.

Network access

An organisation received a call from one of its suppliers, querying when an outstanding invoice would be paid. The organisation confirmed that they had arranged payment of that invoice two weeks prior (via their online payment processing platform) and subsequently shared a remittance advice detailing the same.

Upon review, the supplier identified that the bank account details on the remittance slip were incorrect, which prompted the organisation to investigate.

The investigation first uncovered unusual activity in the organisation's environment via remote access. It was subsequently identified that a Threat Actor had managed to bypass several levels of security to penetrate the organisation's online payment processing platform. At that point, the Threat Actor updated the bank account details for the supplier in question, meaning that the invoice had been paid out to the Threat Actor's fraudulent bank account rather than the supplier's legitimate account.

Deep Dive Topic 5: Claims Trends

Having deep dived into ransomware, BEC incidents, third party breaches and other incident types, here are the headlines based on our observations across all incident types.

Incident spotting

The Analysis Period was dominated by BEC and ransomware incidents, constituting 81% of the total matters analysed.

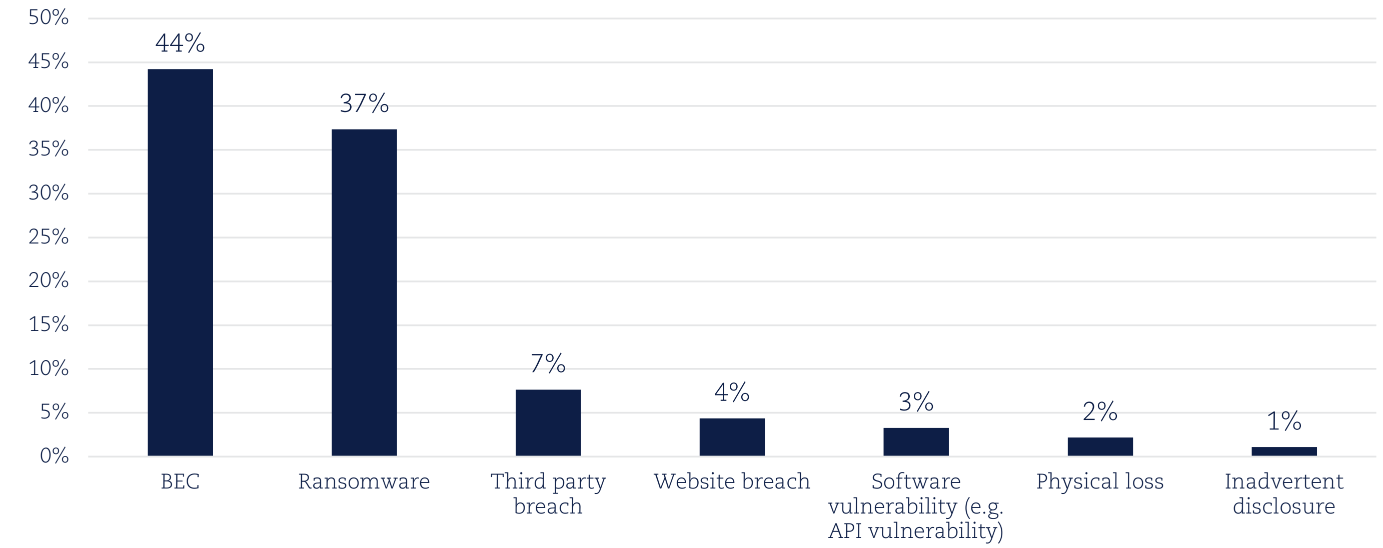
Though their prevalence fluctuates quarter-to-quarter, these incident types are our bread and butter, so to speak.

Third party breaches are on the rise, imploring organisations to jointly investigate breaches, and satisfy themselves of the cyber security practices and posture of those vendors they rely upon.

A collective response is critical in circumstances where personal information is 'jointly held' by an organisation and a third party; it is important to remember that the breach of a third party may give rise to legal and regulatory obligations for joint information holders whose systems may not be involved. This applies to both in the context of privacy obligations (including notifying affected individuals), and in respect of non-privacy regulators (such as ASIC and APRA) where supply chain risk is a key focus.

Though the less common incident types appear to present less of a risk, their impact should not be underestimated. It is critical for organisations to understand their risk exposure including for supply chain vendors that hold data and/or access systems.

Incident type distribution



Sectors impacted

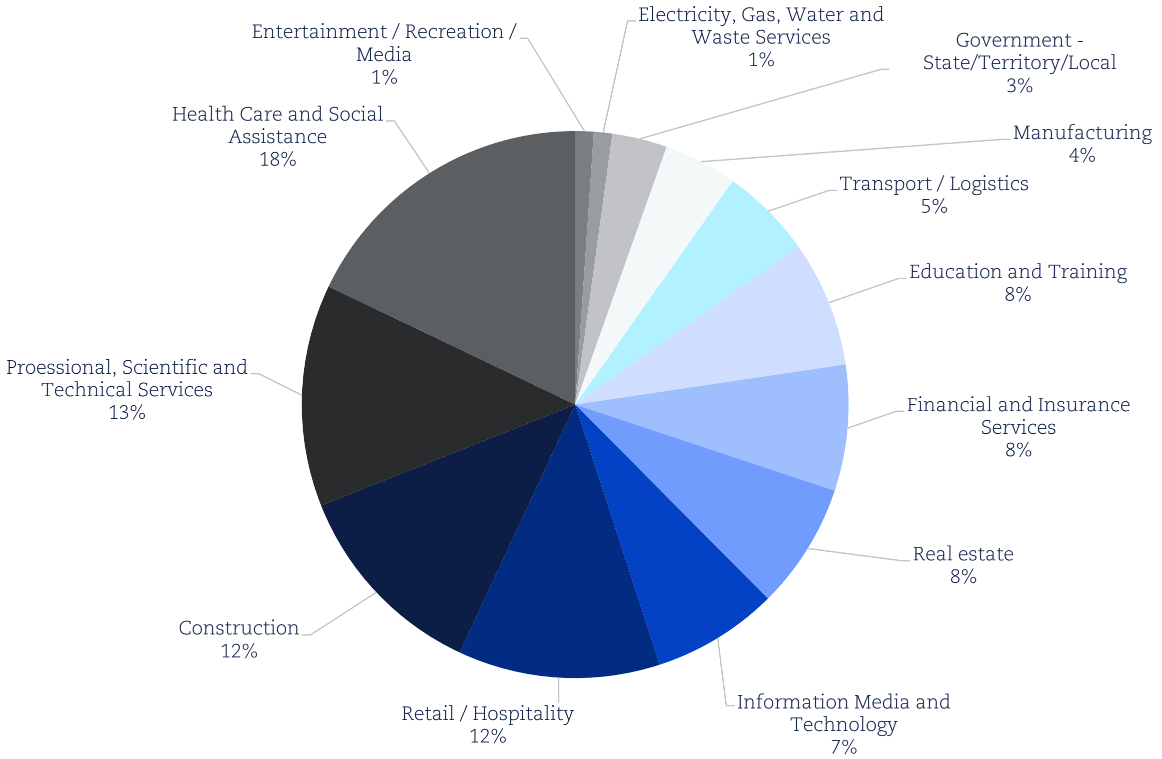
Across the board, the following sectors are most impacted by cyber incidents:

- health services;
- professional services;
- financial services;
- real estate; and
- construction.

This aligns with the OAIC's Notifiable Data Breaches report for notifications made to the OAIC between **1 July** and **31 December 2022**, which highlights that health service providers ***"have consistently reported the most data breaches of all sectors since the NDB scheme began"***.[32]

It is important to note, however, this does not neatly align with those sectors most impacted by the incident types analysed in this Guide (which only focuses on a sample of incidents in the defined Analysis Period) – see further detail below.

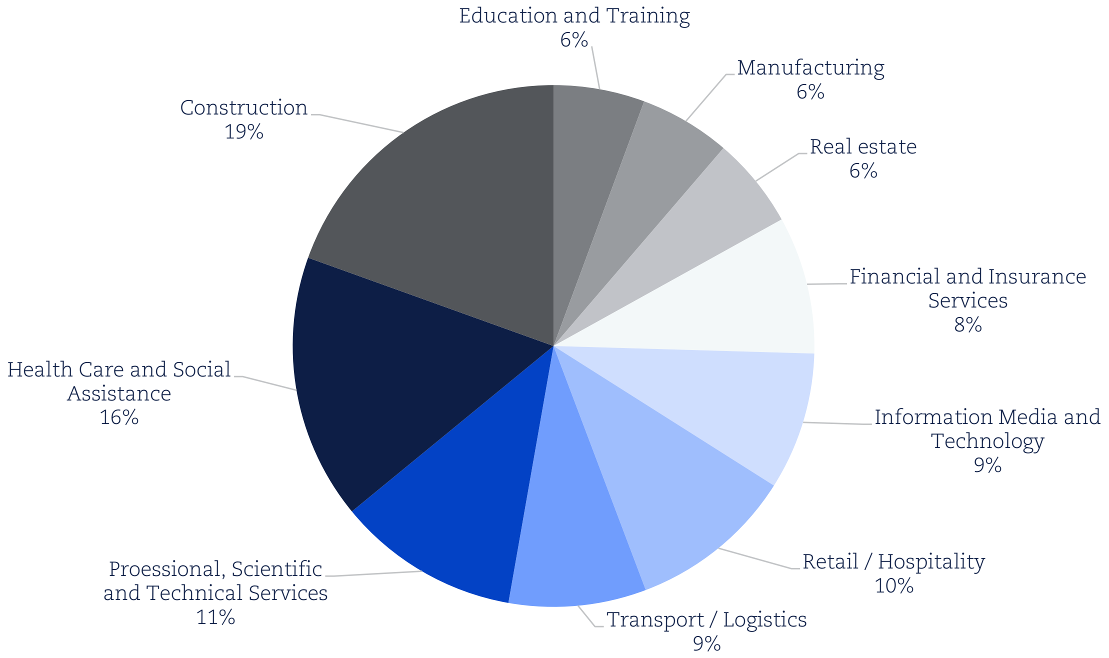
Targeted Sectors - General Breakdown



Ransomware – top targeted sectors

During the Analysis Period, the construction and healthcare were the most commonly targeted sectors by ransomware Threat Actors.

Targeted Sectors – Ransomware



The construction industry is likely appealing to Threat Actors, as the sector has a low threshold for operational disruption; in an industry where on-time deliverables are crucial, any delays caused by ransomware attacks presents a powerful risk. The industry is also perceived as having a more traditional business model, which to a large extent, is yet to implement advanced cybersecurity solutions across the board.

Over the Analysis Period and into the second half of 2023, we have seen a steady increase in ransomware incidents targeting the healthcare industry.[33] The healthcare sector by nature holds significant amounts of health data, considered to be 'sensitive information' under the Privacy Act 1988 (Cth) (**Privacy Act**).

In practice, this means stricter obligations apply and ransomware attacks against healthcare organisations require complex decision making around paying a ransom to avoid publication of the sensitive personal information held. The type of information held, combined with the low threshold for operational disruption that could impact the health of individuals, makes this sector an attractive target for ransomware.

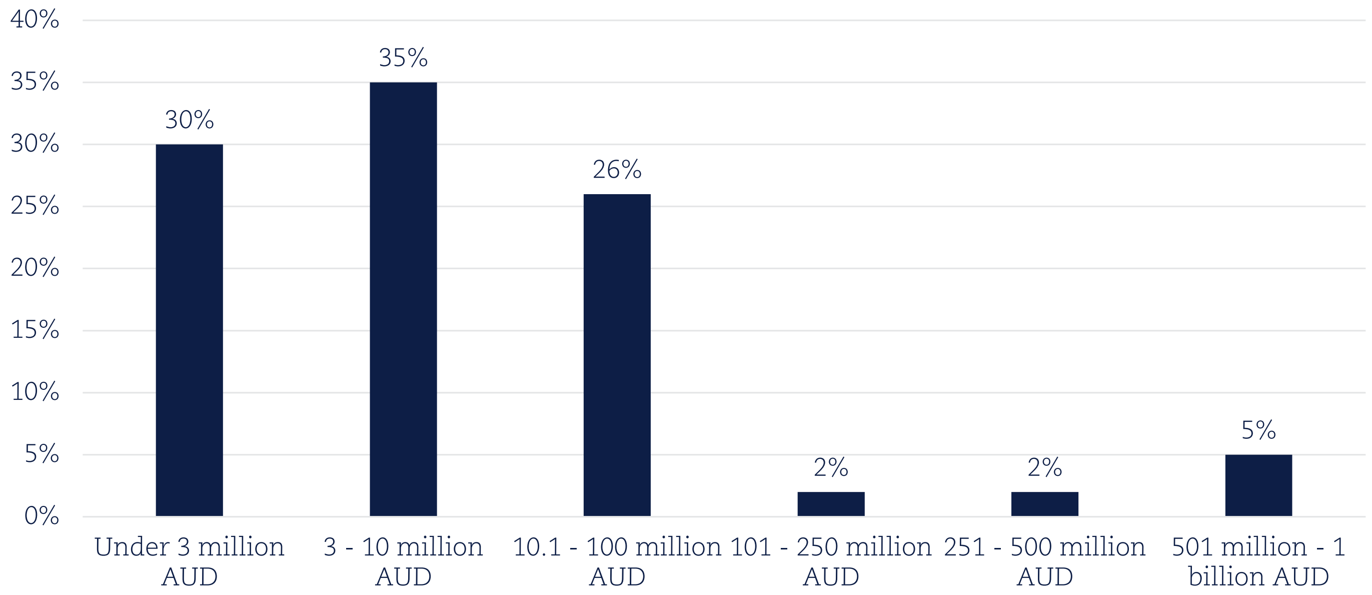
We have a small business problem

Though there are no consistent definitions across government, the ATO defines:

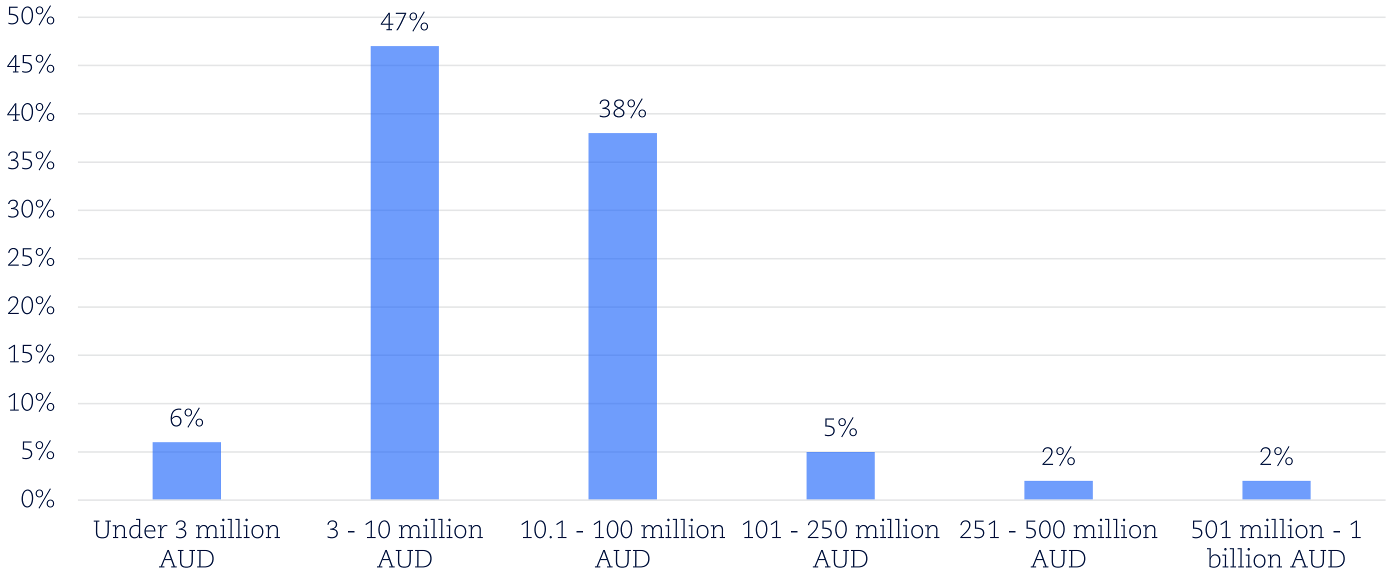
- small business as: a business with a turnover under $10 million AUD;[34] and
- medium business as: companies with a group turnover of between $10 million AUD and $250 million AUD.[35]

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

BEC – Turnover of organisations impacted during the Analysis Period



Ransomware – Turnover of organisations impacted during the Analysis Period



We believe this is where the true risk of cyber-attacks lie, especially given that we are a nation of small businesses (91.9% of businesses in 2022-2023 having a turnover of less than $2 million AUD)[36] and the relatively limited cyber maturity level of organisations (given resource constraints).

How much do cyber incidents cost organisations?

We get this question all the time – how much do cyber claims cost?

There are plenty of resources online from insurers[37] and the oft-cited IBM Cost of a Data Breach Report,[38] which sets out this in detail. We flag that most of this data is US / MENA centric and may not always reflect the Australian experience.

However, we have attempted to capture this information, by calculating the various heads of costs for engagements being:

- IT/Forensic costs;
- legal costs;
- PR costs; and
- notification costs.

We have excluded FTF losses (captured in detail above), defence costs for claims / investigations, any liability / settlement, ransom payments and business interruption losses. We note however, that these heads of loss typically account for the bulk of losses from ransomware incidents for example, with some anecdotally estimating that business interruption, ransomware payments and liability exposure alone can account for 70% of all cyber claim losses.

Across the incidents analysed as part of this Guide, the average cost relating to a cyber incident sits at $233,332 AUD (ex GST – for the purposes of this section of the Guide, all figures reported are exclusive of GST). This figure is, however, skewed by the 21% of matters in which costs exceeded $250,000 AUD, with the median cost of an insurance claim being $71,000 AUD. It also reflects the profile of clients being mostly small to medium sized businesses.

Naturally, smaller incidents cost proportionately less, particularly where containment measures are effective at stopping Threat Actors from doing their worst.

On the flipside, larger incidents typically cost significantly more than these amounts noted above (typically in the millions AUD). One of the major factors that drive costs and losses up is extended systems outage. Being able to restore systems quickly, effectively communicating through a breach, and resorting to tested business continuity solutions is a major factor on mitigating claims losses.

Third party liability exposure is another hidden factor – while cyber losses are typically made up of 'first party costs' (i.e. response costs), 'third party liability' exposure from regulatory investigations, privacy breach claims, B2B recovery actions, and class actions, are continuing to increase. Based on trends we have observed from overseas jurisdictions (including the US and the UK), we expect this will continue to rise and in certain cases dominate the overall loss exposure. This is particularly seen where there is a supply chain disruption or where an industry wide multi-party data breach notification campaign occurs.

Recent public reporting from ASX entities which have experienced major ransomware events demonstrates that cyber losses can extend upwards of $100 million AUD for large loss events. This is without calculating the defence costs associated with running longstanding litigation and regulatory investigations over many years, and does not account for fines and penalties which is an emerging potential head of loss for cyber claims.

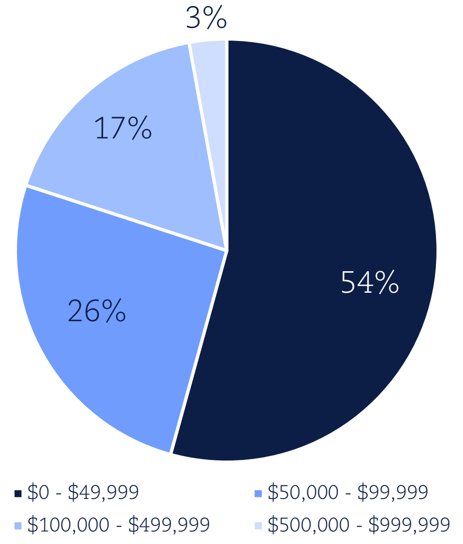
Beyond this, a major determining factor for costs is how much data is stolen, the scope of notification requirements and post-notification support provided to affected individuals, and the ability of a victim organisations to leverage in-house resources to support its response (despite this potentially contributing to operational disruption as key resources are diverted from ordinary day to day activities).

Of course, the necessity of different workstreams in each cyber incident differs and is generally determined by the circumstances of an incident itself. However, as a rule, the value of a claim will almost always surpass an organisation's deductible (except typically for attritional low scale privacy incidents handled in house by say large corporates with sizeable deductibles).

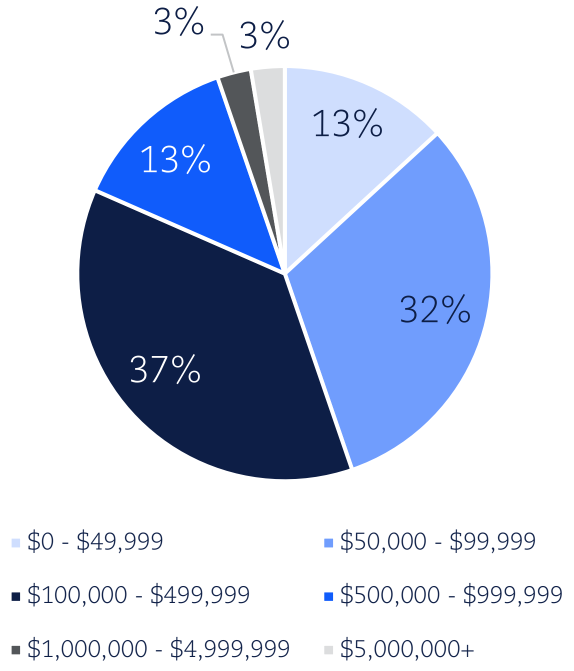
Below, we visualise the total cost of BEC and ransomware matters analysed as part of this Guide. You will see that:

- for small loss incidents: 80% of claims for BEC incidents and 45% of claims for ransomware incidents (which collectively form 81% of matters analysed) come in at under $100,000 AUD; and
- for larger loss incidents: 3% of claims for BEC incidents exceed $500,000 AUD and 3% of ransomware incidents exceed $5 million AUD.

Total cost of claim (AUD) - BEC incidents



Total cost of claim (AUD) - ransomware incidents



The role of insurance in the cyber industry

In the early years, if your organisation wanted a cyber insurance policy, all it had to do was satisfy two questions – Do you have a computer? Tick. Is the computer connected to the internet? Tick.

Fast forward to 2024, and the hoops that organisations are required to jump through in order to be eligible for cyber insurance are extensive. That said, in our experience the security control uplift process that many organisations must go through to get 'insurance ready' has multiple upsides.

This is where the Strategy should work to improve its understanding of the value of the insurance industry to force multiply the strategic requirements it is intending to achieve. Insurers understand cyber risk, and how to overcome those risks. In working with brokers who act as a trusted adviser, the insurance industry can be leveraged to force multiple key messages across the industry (small, medium, and large-scale organisations).

On the ground, we are seeing the insurance industry do just this.

First, by increasing security control requirements alongside purchasing cyber insurance, insurers and brokers are ensuring that organisations are inherently less attractive as a target, simply because they no longer represent an easy win for Threat Actors.

Secondly, insurance requirements are often aligned to government standards, meaning that organisations can effectively 'kill two birds with one stone' – become cyber insurance fit, and meet industry best practice requirements. This includes preventing and preparing for an incident.

Thirdly, unlike many other insurance policies that simply offer balance sheet protection (although it does that too), the cyber insurance solution is designed to provide both:

- **a promise to protect** – many insurers are investing in commercial tools to stop Threat Actors at the gate, including vulnerability scanning and remediation solutions, dark web scanning and credential exposure remediation support, and critical vulnerability patching alerts; and

- **a promise to respond** – insurers have conducted due diligence on the incident response market and assembled teams that do breach response daily. In practice, these teams are on standby to support for policyholders, supplement their internal capabilities, and provide surge capacity for large loss events across multiple fields of expertise. Insurance rates are typically 40% less than corporate rates, meaning that policyholders get more from using cyber insurance panel vendors than if they paid corporate rates of traditional service providers. This, in turn, enables policyholders to take their deductible contribution and their limit of liability further before self-funding breach response efforts.

Combining these factors, what we end up with is independent validation from third party insurers that manage risk across the globe and can spot trends and help their policyholders to respond accordingly. Many large corporates are looking to lean on their insurance solution and maximise the support available through it. Many corporates have recently seen the value in cyber insurance as a retainer service as well as a backstop for financial loss reimbursement.

In our experience, this is highly effective in bringing together risk managers, the C Suite, and Boards, to open doors for approval of priority items and mitigate risk. CISOs and MSPs can gain more from using cyber insurance as leverage to give an independent voice to validate their concerns. For example, we often hear of budgets being approved for cyber uplift projects off the back of the C-Suite being told that they can't obtain insurance due to not meeting minimum standards.

All of that being said, while we believe that cyber insurance is an incredibly important tool for the maturity of the corporate sector, we recognise that small businesses often lack the resources, money, or time required to go through an expensive uplift process.

In practice, we appreciate that the underwriting process can be overly onerous and confusing for small businesses, and on occasion, act as a barrier for purchasing insurance.

While we believe there are varying approaches that can be adopted to support the smaller end of the market from an insurance perspective, we also consider that the Strategy can play an important role in helping SMEs uplift their cyber security and response capabilities.

Proportion of insured events

The World Economic Forum has reported that only 25% of SMEs carry cyber insurance.[39] This is also assuming a revenue of <$250 million USD which for Australia, would represent a relatively large-scale operation. It is hard to identify the exact number of SMEs that buy cyber insurance, with the Insurance Council of Australia estimating the number is closer to 20%.[40] Anecdotally, within the insurance industry, the number is estimated to be probably closer to 10-15%.

The impact of a cyber incident on any organisation can be devastating, however this is particularly so for SMEs.

Noting the cost of effectively responding to a cyber incident, as outlined above, we have seen firsthand the impact on SMEs who:

- are uninsured; or
- have a high deductible, and have not self-funded the possibility of a cyber incident in budget allocations.

This includes in a handful of cases, the looming prospects of bankruptcy but for insurance being available to carry over losses for response costs and business interruption. We have seen firsthand Boards operating in safe harbour while trading in distressed circumstances and have recently seen a company shut down because of trading losses following a cyber-attack. While these cases are relatively rare, they do exist.

In our experience, regulators (and consumers) do not consider lack of insurance or prohibitive costs a sufficient excuse for organisations inadequately responding to a cyber incident.

This places uninsured organisations at a disadvantage, noting an effective response to a cyber incident must be timely and proportionate. This comes at a cost, often leaving a gap in incident response quality.

Given the nature of our practice, approximately 70% of our clients are insured (30% being uninsured), however this does not align with insurance rates across the market.

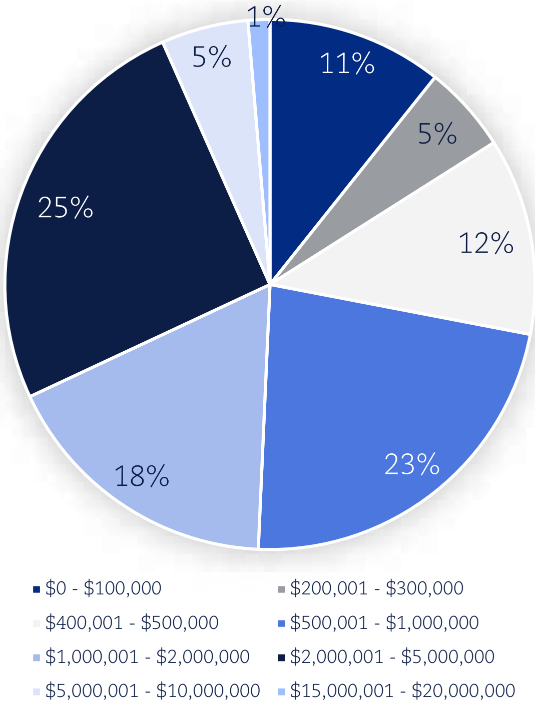
We also note that of the 70% insured organisations, a proportion are large corporates who engage us directly even if the overall breach response costs (IT / forensic costs etc) do not exceed their deductible. We still count these as insured incidents despite the response not leading to an insurance claim being made.

Considering this through the lens of the Strategy, we consider there is an opportunity for government to further promote the uptake of cyber insurance as a tool to help organisations effectively respond to cyber events

Policy limits and deductibles

Policy limits

Of those entities with cyber insurance in place, the average policy limit sits at approximately $2.5 million AUD, whereas the median sits at $1 million AUD.

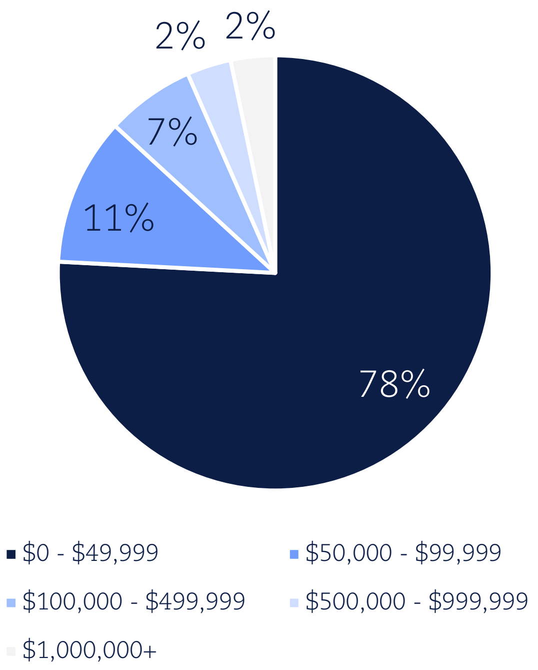


Depending on the nature of an incident, we work with organisations to determine what work can be completed within these limits by all vendors, and assist them with undertaking additional work in-house to reduce costs in instances where their policy limit has been/will be reached.

Deductibles

Across the Analysis Period we observed an average deductible of approximately $50,000 AUD, and a median of $5,000 AUD. These are generally proportionate to the size of the organisation and their insurance program specifications.

In the majority of cases, the deductible is eroded either in whole or in (large) part by IT recovery / forensic investigation costs (which, across the incidents analysed, ranged from $3,240 AUD to over $600,000 AUD – averaging approximately $63,000 AUD).



Does insurance pay?

Of the incidents experienced by organisations with cyber insurance, we see an extremely marginal declinature rate (quite literally a handful amongst thousands). This supports our experience that cyber insurance does exactly what it says on the tin – it provides cover to organisations for responding to cyber incidents.

This is contrary to the common headlines that suggest 'insurance doesn't pay'. In our view, these headlines are unhelpful and do not reflect the true state of the cyber insurance claims market which exists to support clients and pay claims.

Cyber cover is drafted to be intentionally broad. In instances where coverage issues do arise, this is most likely due to gaps in expectations of how different policies are intended to respond.

Organisations should speak to a specialty insurance broker to understand their policies and the extent to which they provide cover for cyber incidents. In our experience, a standalone cyber insurance policy is generally the only way to guarantee cover, with additional conversations being around whether FTF losses and business interruption losses are sufficiently covered.

How long does it take to respond to an incident?

The time between first access by a Threat Actor and discovery of an incident by an organisation often correlates with the severity of the incident, scope of lateral movement, volume of data exfiltrated, number of individuals impacted, length of regulatory engagement, and in turn, the cost and effort required in response.

In an ideal world, incidents would be identified, contained and remediated within hours. However, there are numerous factors at play here including an organisation's ability to detect and respond to active threats.

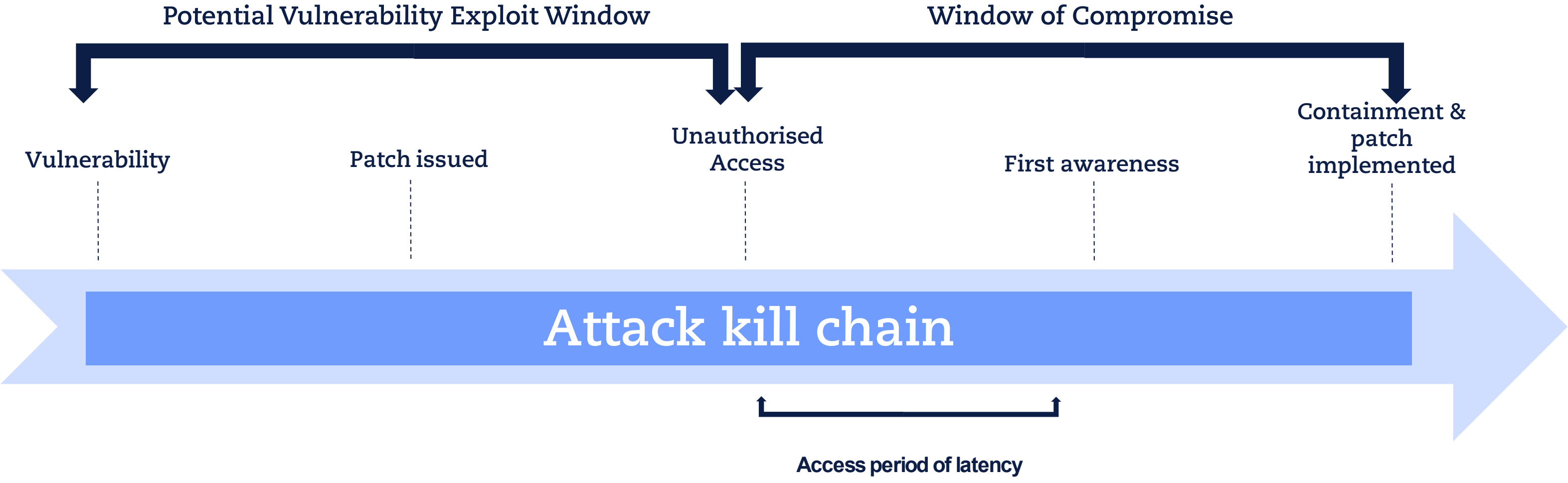
Discovery of an incident will often 'start the clock' in terms of an organisation's regulatory and disclosure obligations. The less time a Threat Actor has been in an environment, the less complex the investigation required, and thus the faster an organisation can close out its response to a cyber incident.

Attack kill chain – detection latency

In reality, there is often a delay between the Threat Actor gaining unauthorised access to an environment, and the organisation becoming aware of the unauthorised access – we refer to this as the 'latency period'.

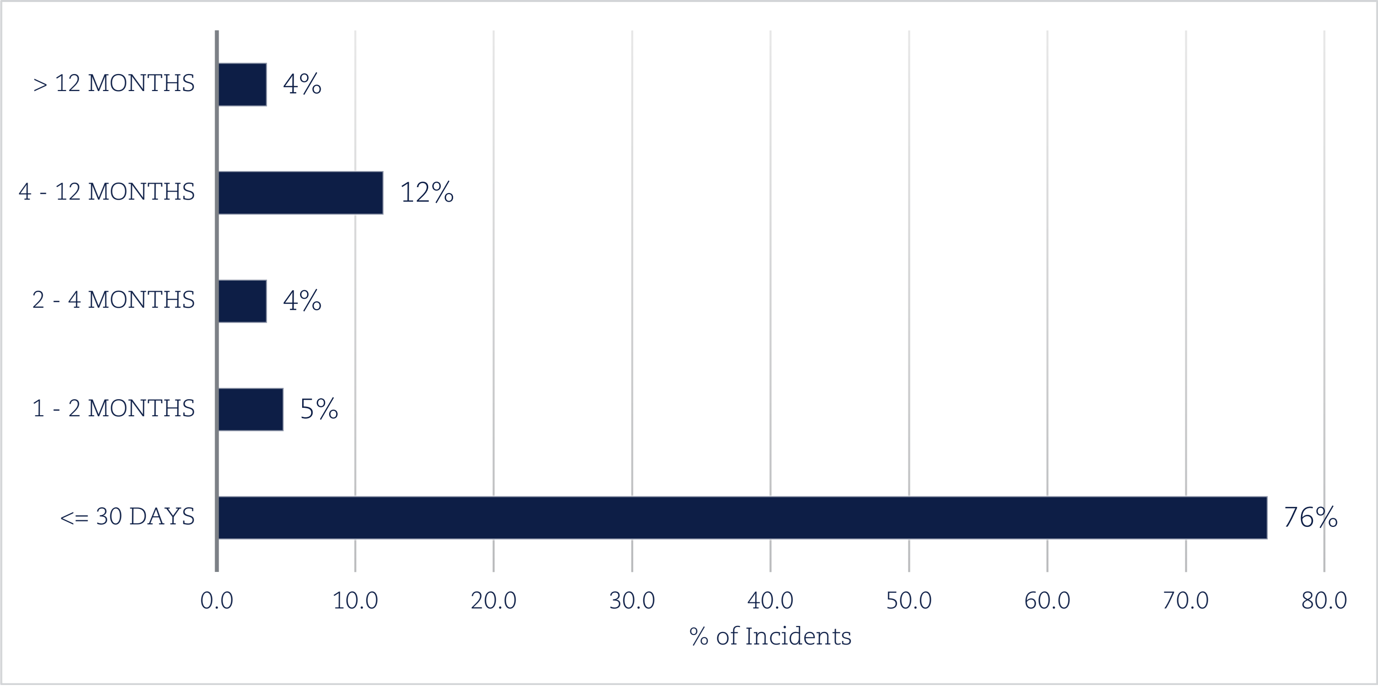
For example, it is common for a Threat Actor to be in an organisation's environment for an extended period of time before the organisation is alerted to their presence (for example, deployment of malware, a ransom note or redirection of emails). Our data shows that the median number of days taken for organisations to detect the presence of a Threat Actor is 5 days, while the average is 49 days. The average is considerably higher, taking into account the incidents where it can take hundreds of days to detect the presence of a Threat Actor. However, even five days is generally enough time for a Threat Actor to steal a considerable amount of data, delete backups and commit fraudulent acts.

Positively, we have seen the latency period has considerably decreased from previous years, as advanced threat detection tools are getting better at picking up threats. Across the Incidents in the Analysis Period, 31% of organisations experiencing a BEC and over 40% of organisations experiencing a ransomware incident identified the Threat Actor within one day of initial unauthorised access, with 78% of organisations experiencing a BEC and close to 84% of organisations experiencing a ransomware incident identifying the Threat Actor within 30 days.

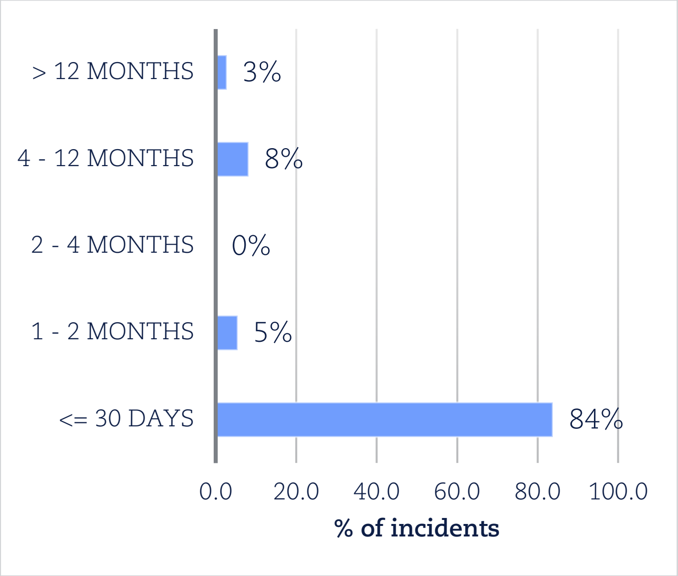


Median window is 5 days, while average window is 49 days between initial unauthorised access and first awareness.
Average reflects those incidents where the Threat Actor goes undetected for extended periods of time (i.e. hundreds of days).

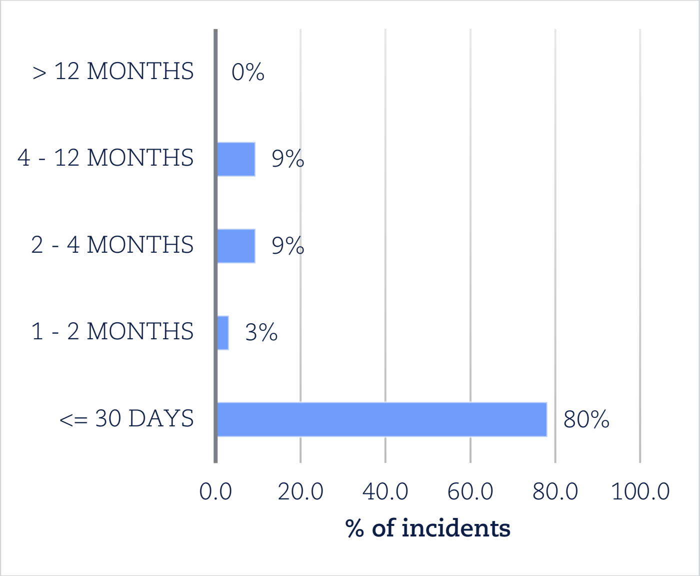
Latency - All incidents



Latency - Ransomware incidents



Latency - BEC incidents



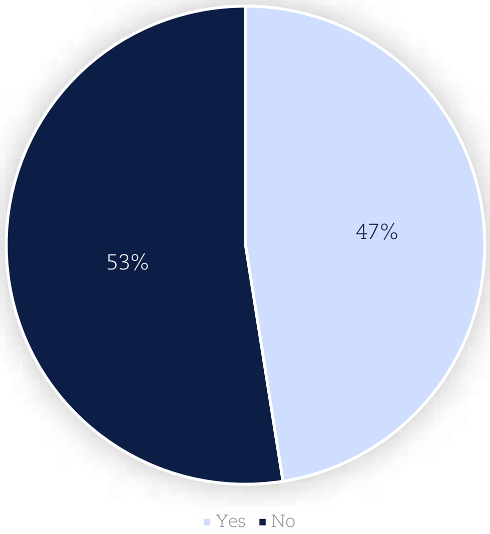
Notifications

Regulatory notifications

Across the Incidents in the Analysis Period, 47% of the Incidents were notified to a regulator, including;

- 42% of incidents being notified to the OAIC; and
- 5% of incidents being notified to another regulator (including ASIC, APRA and/or others).

Incidents that were Notified to a Regulator



The threshold for notification to the OAIC also only applies to APP Entities generally with an annual turnover of more than $3 million AUD (subject to some exceptions). In other words, an AFSL Licensee, for example, may be required to report a cyber incident as a *'reportable situation'* to ASIC, however may not be required to report the same incident to the OAIC if their annual turnover is less than $3 million AUD. Specific legal advice is clearly required in each case.

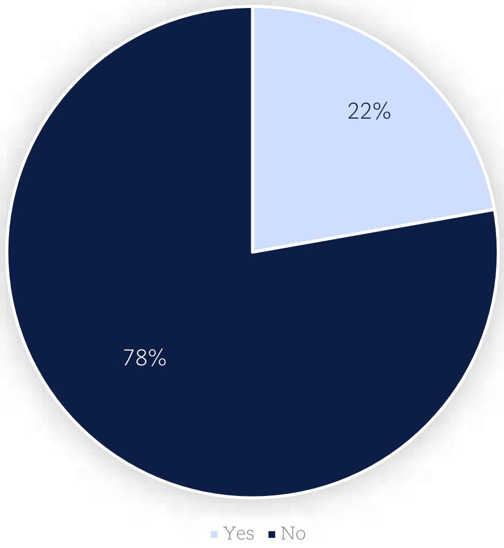
In the current climate, organisations notifying incidents to the regulator should brace for increased scrutiny, particularly where they have experienced a prior incident or have clearly breached the Australian Privacy Principles (**APPs**) (for example, where an organisation has retained personal information for longer than permitted, and this information has been impacted by a breach).

As above, the thresholds for notification to different regulators and the ASX differ, so must be considered in their own right. As a general rule, a cyber-attack that would reasonably be expected to have a material effect on the price of a listed entity's securities are required to be disclosed to the ASX.

We have seen that of those ASX listed entities that had an incident during the Analysis Period, 22% notified the market. While this aligns with recent reporting from ASIC through the Australian Financial Review[41], we also note that not all of the incidents impacting ASX listed entities during this period were considered serious cyber security breaches. There were also a mix of incident types – ransomware and BECs.

Not every cyber incident will necessarily require market disclosure, and there are multiple factors that Boards will consider in meeting their obligations in this respect. Advice should be sought from those with experience understanding materiality thresholds in the context of cyber incident investigations – this space is a quickly evolving and requires careful considerations to manage both market and general crisis communications concurrently.

Incidents Notified to ASX



Number of individuals notified and number of potential individuals impacted

We have been closely tracking the evolution of what is considered 'serious harm'. So to has the OAIC, who now expects reporting entities to disclose the gap between the number of individuals whose personal information is involved in a data breach, and the number of individuals who are ultimately notified of a breach.

The legislative threshold for individuals requiring notification is set out in the Privacy Act and requires the impacted organisation's assessment as to whether any individuals are at a resulting risk of 'serious harm' by reference to numerous factors, which are broadly categorised below:

- the type or types of personal information involved in the data breach – this includes a consideration of the kind and sensitivity of the information at risk;
- the circumstances of the data breach – this includes a consideration of the kinds of persons who have or could obtain the information; and
- the nature of the harm that might result from the data breach – this includes a consideration of the likely type of harm that could flow as a result of the access to information including potential physical, psychological, emotional, financial or reputational harm.

These factors must also be combined with additional considerations noting recent high-profile breaches, including:

- how to notify, including whether notification would cause undue alarm (for example, whether an individual has any inherent vulnerabilities that need to be considered);
- the rolling ***"notification fatigue"*** occurring from a high proportion of the population being impacted by and notified of cyber incidents in the past 2 years; and
- the 'mosaic effect', being that "every piece of data that is compromised can increase the likelihood of cyber actors linking together pieces of information to gain insight or do harm" giving Threat Actors ***"the ability to more easily impersonate an individual or access systems or accounts using compromised credentials".*** This has been recently highlighted by the finding of the 'mother of all breaches' dataset online by security researchers – some 26 billion records combined.[42]

In other words, the effect of recent high-profile and widespread cyber incidents is that individuals that would otherwise not have met the 'serious harm' threshold may do so if their personal information has been impacted by multiple incidents.[43]

Consideration needs to be given to post-notification support to encourage affected individuals to take self-protection measures to prevent data misuse.

The road ahead – where to focus your energy in 2024

We often see in incident response that organisations can feel powerless – fighting a force much greater than their own, enduring a never-ending process laden with challenges, risk and uncertainty.

The good news is, it doesn't always have to feel that way.

With cyber incidents gaining attention and momentum in the last few years, we have observed a significant uptick in general willingness of Australian organisations to look at themselves in the mirror, identify gaps, and invest in tools that can boost their cyber resilience.

Whether you're well on your way or just starting out on this journey, we have identified the top items that we think make a real difference to the battle against cyber criminals and better prepare your organisation to decisively respond to cyber-attacks.

Most of these items are in response to what we call 'severity factors' – i.e. factors which amplify the impact of breaches on the organisation, affected individuals, and the bottom line.

Feel free to use this to list to guide what you can focus on in 2024. Of course, you should seek your own advice from industry professionals if you want to develop a cyber-risk maturity strategy that is tailored to your organisation, beyond the items listed here.

Get to know your incident response partners and processes

Whether you have cyber insurance or not, in building your incident response bench you should get to know the team who will be there on the day. This includes introducing your external team to each other, and clearly establishing roles and responsibilities particularly where there is a cross-over of core and non-core services.

Ensuring vendors do not trip over each other in trying to support the victim organisation (however well intentioned) is key to an efficient and effective incident response. Understanding internal capabilities and supplementing them with cyber insurance support options should also be explored.

The easiest way to do this is to identify which vendor will manage which incident response 'workstream'. Some examples of the key workstreams are:

- incident response management (also referred to as 'Breach Coaching');
- legal/regulatory advice;
- cyber insurance management;
- communications;
- Threat Actor management;
- IT containment and forensics; and
- IT systems recovery.

If you have cyber insurance, you should contact your broker to organise a complimentary 'meet the breach coach' session.

You've bought cyber insurance – lean into the service and make it work for you. This includes mapping out the process for activating the breach response service which sits behind the insurance policy (which is entirely separate from making an insurance claim). Too often we see process unfamiliarity slow down the breach response lifecycle at critical early stages.

Finally, when it comes to notifying insurers, we often see incident response plans assign this action only when an insurance claim is to be made. Rather, the cyber incident hotline should be contacted as soon as practicable upon suspecting a cyber incident.

In other words - treat your insurance policy exactly like you would use a retainer with your usual incident response provider. If you are calling them you should be calling the hotline at the same time.

Control and process uplift and remediation

There are many free resources and paid services available to better understand whether the controls your organisation has in place are appropriate and right-sized to protect your data, the continued operations of your systems, and to prevent cyber-attacks.

This includes consulting with your usual cyber risk advisor or cyber insurance broker to obtain the latest information about cyber-attack threat mitigation, and signing up to government resources such as the Cyber Wardens program, ACCC's Scamwatch, ACSC and other alerts.

However, this year, if we are to reduce the severity factors which have contributed to a notable 2023, a key focus will be on implementing controls to prevent the following:

- **FTF** – including reinvigorating the drive for MFA for financial controllers' systems (both email and payment systems), introducing MFA fatigue training for all critical staff, and reinvigorating call back procedures where financial controllers have delegated authority to process and authorise payments;
- **supply chain risk management** – including better understanding, uplifting and testing capabilities of third parties that jointly hold data or have administrative access to systems. This includes bolstering requirements and aligning on processes for how organisations will jointly assess, mitigate and notify data breaches; and
- **counter-ransomware measures** – although we are heading in the right direction as an industry, we can't be complacent. To ensure ransomware numbers keep heading in the right direction, it is vital that we keep on top of the latest exploited vulnerabilities, system access trends, and implement enhanced detection and response capabilities.

Effective data management

Data was once considered 'gold' for businesses – the key to unlocking key insights and efficiencies. Recent major data breaches have demonstrated that data is perhaps better considered 'uranium' – an asset, yes – but also a liability if not properly stored and managed.

The retention of too much data has unequivocally been the largest severity factor for recent major data breaches. Although this is arguably not a new issue, it has been reemphasised in 2022-3 as something to be critically addressed. To reduce their data footprint and corresponding exposure levels, organisations should conduct:

- **data audit** – a review of the types of data you hold, where it is held and who by, 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 / classification** – an assessment of your legal obligations regarding the retention of data, which should include a review of relevant data retention policies and standards to ensure there is a clear and workable framework to continuously review data management, as well as consideration of whether there are ways you can better store data, especially if it is not in active use (including consideration of encryption or archival options);
- **data deletion** – where possible, deletion of data not required, including in production and non-production environments (backups, cold storage etc). This should include a review of data held by external employees and vendors, especially with the rise of third-party data hosting; and
- **training** – it is no longer enough that relevant policies and procedures exist. Employees need to be empowered and trained on the policies, processes and procedures for effective data management. This includes the regular detection and remediation of off-policy behaviour.

Train and test your Incident Response Plan (IRP), CMT and Board

Cyber crisis exercises have been popular well before cyber became a prominent issue. Typically, these exercises were conducted by the IT team (red teaming) or through a Business Continuity lens. In 2024, it is now clear that cyber requires more than just an IT-level response, and it is vital that Executives, Boards and authorised decision makers are prepared for the worst and have rehearsed their approach to cyber incident response. This is echoed in regulatory guidance from ASIC, APRA and the OAIC, and is often a requirement to operate in key sectors.

Cyber crisis exercises and simulations continue to grow in popularity and most ASX entities would have completed exercises over the last 4 years. We highly recommend ensuring that at least the crisis management team (**CMT**) (or equivalent) conduct at least one cyber readiness exercise per year, to b well-rehearsed during 'peace time', so they can perform effectively during 'war time'.

Examples include (in increasing level of maturity):

- **Tabletop Exercise** – a discussion-based exercise that offers an informal operational environment for team members to build their understanding of the incident response process.
- **Cyber Simulation** – participants experience a hypothetical cyber incident as it unfolds in semi-real time to develop muscle memory and practice effective response using the actual structure of the CMT (or equivalent).
- **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; IT response and recovery, CMT / Board and Business Continuity Management. It provides the most true-to-life cyber incident response experience.

As well as helping build the vital 'muscle memory' of cyber incident response, these exercises also help:

- **build an awareness** around various cyber incident types, the current cyber threat landscape, and evolving regulatory frameworks to ensure Executives and Directors are up-to-speed on cyber risk and potential exposure;
- **identify opportunities for procedural improvement** by revisiting and enhancing documentation including Crisis Management Plan, Business Continuity Plan, Cyber Incident Response Plan, Data Breach Response Plan, incident-specific playbooks and other Government, Risk and Compliance documentation; and
- **clarify roles and responsibilities** for both internal teams and external stakeholders.

This year, we are recommending that certain industries link up and perform joint exercises with key suppliers and clients to test interoperability and communications requirements.

Communications playbooks

In the past, communications playbooks were always seen as a 'nice to have'. Recent events over the past 18 months have entirely flipped that notion on its head, as communications and operations teams are being recognised as the backbone of the CMT.

We consider that crisis communication preparation is a must-do for 2024. 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.

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).

Cyber insurance – especially for small and medium businesses

This Guide has highlighted the ways in which cyber insurance can help protect businesses as well as help them respond to incidents.

Cyber insurance is an effective wholesale economy wide protection blanket which will move the dial on driving cybercrime down across the SME market, which is a very large part of our economy made up of over two million small businesses.

This is especially if the Small Business Exemption is to be removed from the Privacy Act – making those organisations responsible for protecting data and reporting breaches at a scale never seen before in our economy.

On the flip side, we recognise that organisations may elect not to purchase cyber insurance and rather self-fund against the risks of a cyber-attack. Notwithstanding this, we consider that all of the above points still apply in terms of general steps that can be taken to improve cyber maturity and the ability to respond to a cyber incident.

In other words, even if you don't have cyber insurance you should still go through the process of defining your incident response team, meeting with those key vendors and stakeholders, aligning on processes for engagement and commercial terms, etc, to put your organisation in the best position to respond.

Methodolgy

The aim of this Guide is to provide an accurate overview of cyber risk and the challenges facing Australian businesses today (at least, as we see it).

Having managed over 5,000 incidents globally in the past ten years, we have a keen understanding of the cyber landscape and how to manage cyber risk.
Through sharing our observations and overarching experience, we aim to encourage a frank, fact driven conversation about cyber risk and what we as an industry need to prioritise now to best promote resilience in the future.

The data is also hopefully a reflection of where we have come from, and where we are going as an industry. There is a lot of good news in here as well as points for further consideration both in setting the Strategy and the industry working within the Strategy over the coming years.

Period of collection

The incidents in-scope are taken from 1 January 2022 through to 31 March 2023.

From that period until the date of publication of this Guide, our team has spent time gathering and anonymising the data, uplifting the data to ensure its integrity and accuracy, and collecting additional data from global contributors and sources (including Coveware, and other commercial threat intelligence which we subscribe to).

From there, we have dedicated significant time towards analysing and visualising the dataset, comparing other industry statistics to identify unexplainable deviances, and preparing the Guide.

This timeline has allowed us to provide a complete and accurate picture of key cyber incident trends across the full incident lifecycle.

Categories of data

We analysed 63 data fields across incidents that took place within the above period.

These data fields cover the following key areas:

- incident type;
- incident root cause;
- organisation industry profile and revenue;
- Threat Actor behaviour;
- costs and losses; and
- insurance related data.

Like with any data analysis, there are always statistical biases and we have sought where possible to limit these in our analysis. For example, we have ensured:

- a cross-selection of engagements;
- a cross-selection of vendors (including IT forensic etc); anda
  - mixture of engagements where organisations both had and did not have insurance

Endnotes

[1] Australian Government, Department of Home Affairs, *2023 – 2030 Australian Cyber Security Strategy (Discussion Paper, 22 November 2023) ('The Strategy')*.

[2] Office of the Australian Information Commissioner, *Notifiable Data Breaches Report: July to December 2022 (Report, March 2023) ('OAIC NDB Report Jul-Dec 2022')* 3, 20, 21.

[3] Office of the Australian Information Commissioner, *Notifiable Data Breaches Report: January to June 2023* (Report, September 2023) 18 (*'OAIC NDB Report Jan-June 2023'*) 3, 24.

[4] European Union Agency for Cybersecurity, *ENISA Threat Landscape 2023* (Report, 19 October 2023) 9.

[5] Information Commissioner's Office, *Data security incident trends* (Web page) <https://ico.org.uk/action-weve-taken/data-security-incident-trends>.

[6] Australian Cyber Security Centre, *ASD's ACSC Annual Cyber Threat Report, July 2021 to June 2022* (Report, 4 November 2022) 47.

[7] Australian Cyber Security Centre, *ASD Cyber Threat Report 2022-2023* (Report, 14 November 2023) (*'ACSC Threat Report'*) 38.

[8] SonicWall, 2022 *SonicWall Cyber Threat Report* (Report, 2022).

[9] Athina Mallis, 'Organisations have a lack in trust over board's data governance knowledge', *Digital Nation* (Australia, 8 January 2024); Financial Review, 'Cybersecurity is the No.1 risk not getting the attention it deserves' *Financial Review* (online, 1 January 2024) <https://www.afr.com/chanticleer/cybersecurity-is-the-no-1-risk-not-getting-the-attention-it-deserves-20240101-p5euhv>; The Strategy (n 1).

[10] TrendMicro, Lockbit, Blackcat, and Royal Dominate the Ransomware Scene (Web page) <https://www.trendmicro.com/vinfo/au/security/news/ransomware-by-the-numbers/lockbit-blackcat-and-royal-dominate-the-ransomware-scene-ransomware-in-q4-2022>.

[11] Abnormal, *A Deep Dive into Active Ransomware Groups* (Web page) <https://abnormalsecurity.com/blog/deep-dive-active-ransomware-groups>; Australian Cyber Security Centre, *Understanding Ransomware Threat Actors: LockBit* (Report, 15 June 2023); HelpNetSecurity, *New threat groups and malware families emerging* (Web page) <https://www.helpnetsecurity.com/2022/04/22/adversaries-innovating-and-adapting/>; HelpNetSecurity, *RaaS proliferation: 14 new ransomware groups target organizations worldwide* (Web page, 25 July 2023) < https://www.helpnetsecurity.com/2023/07/25/active-ransomware-groups-2023/> (*'Raas proliferation'*).

[12] Flashpoint, *Breaches and Malware: 2023 in Review* (Report, 28 November 2023); Flashpoint, *Insider landscape 2023 in Review* (Report, 12 December 2023); Intel471, *Threat Brief – Q1 2023 recap: Russia's ware in Ukraine a year on, developments in artificial intelligence, ransomware, access offers, malware, vulnerabilities* (Report, 5 April 2023); Intel471, *Threat Brief – Q4 2023 recap: Varied hacktivism, persistent ransomware activity, drop in access offers, tenacious malware operations, new vulnerabilities* (Report, 18 January 2024).

[13] Joint Cybersecurity Advisory, '*Understanding Ransomware Threat Actors: LockBit'* (Media Release, 14 June 2023); HelpNetSecurity, *New threat groups and malware families emerging* (Web page, 22 April 2022) < https://www.helpnetsecurity.com/2022/04/22/adversaries-innovating-and-adapting/>; *Raas proliferation* (n 11).

[14] Australian Cyber Security Centre, *2023-03: ASD's ACSC Ransomware Profile – Lockbit 3.0* (Web page, 20 March 2023) <https://www.cyber.gov.au/about-us/advisories/2023-03-asdacsc-ransomware-profile-lockbit-3.0 >.

[15] The Hacker News, *The Prolificacy of LockBit Ransomware* (Web page, 14 March 2023) < https://thehackernews.com/2023/03/the-prolificacy-of-lockbit-ransomware.html>.

[16] The Strategy (n 1) 22.

[17] Coveware, *Ransomware Threat Actors Pivot from Big Game to Big Shame Hunting* (Report, 3 May 2022); Coveware, *Fewer Ransomware Victims Pay, as Median Ransom Falls in Q2 2022* (Report, 28 July 2022); Coveware, *Uber Verdict Raises New Risks for Ransom Payments* (Report, 26 October 2022); Coveware, *Improved Security and Backups Result in Record Low Number of Ransomware Payments* (Report, 20 January 2023).

[18] ACSC Threat Report (n 7) 34, 39.

[19] Federal Bureau of Investigation, *Internet Crime Report* (Report, 2022) 11.

[20] Chainalysis, *2023 Crypto Crime Report,* (Report, February 2023) 27.

[21] Australian Competition & Consumer Commission, *Targeting scams: report of the ACCC on scams activity 2022* (Report, 17 April 2023) (*'ACCC – Targeting scams'*) 13.

[22] Australian Payment Network, *2022 Australian Payment Fraud Report,* (Report, 2022) 11-12.

[23] ACCC – *Targeting scams* (n 19) 13.

[24] National Anti-scam Centre, *Targeting scams report* (Report, April 2023) 13.

[25] ACSC Threat Report (n 7) 39.

[26] James Purtill, '*Australia's overheated property market has become a target for hackers – and they're scamming millions' ABC News* (online, 24 April 2022) <https://www.abc.net.au/news/science/2022-04-24/scammers-hackers-real-estate-deposit-property-settlement/101000288>

[27] OAIC NDB Report 2023 (n 3) 29.

[28] Australian Bureau of Statistics, *Characteristics of Australian Business* (Report, 4 June 2021).

[29] National Cyber Security Centre, *'MOVEit vulnerability and data extortion incident'* (Web page, 27 June 2023) <https://www.ncsc.gov.uk/information/moveit-vulnerability>

[30] IBM, *Cost of a Data Breach Report 2023* (Report, 2023) (*'IBM – Costs of Data Breaches'*) 23.

[31] ACSC Threat Report (n 7).

[32] OAIC NDB Report Jul-Dec 2022 (n 2) 27.

[33] Kim S. Nash, *'Surge in Hospital Hacks Endangers Patients, Cyber Official Says'* WSJ Pro Cybersecurity (Australia, 7 September 2023).

[34] Australian Taxation Office, *Latest estimate and trends* (Web page) <https://www.ato.gov.au/about-ato/research-and-statistics/in-detail/tax-gap/large-corporate-groups-income-tax-gap/latest-estimate-and-trends>.

[35] Ibid.

[36] Australian Bureau of Statistics, *Counts of Australian Businesses, including Entries and Exits* (Web page) <https://www.abs.gov.au/statistics/economy/business-indicators/counts-australian-businesses-including-entries-and-exits/latest-release#turnover-size>.

[37] Net Diligence, *Cyber Claims Study* (Report, 2023); Chubb, *Chubb Cyber Index* (Web page) <https://www.chubb.com/au-en/business/cyber-claims-data.html>.

[38] IBM – Costs of Data Breaches (n 28).

[39] World Economic Forum, *Global Cybersecurity Outlook 2024* (Report, 11 January 2024) 9.

[40] Insurance Council of Australia, *'Cyber risk'* (Web page) <https://insurancecouncil.com.au/issues-in-focus/cyber-risk/>.

[41] Patrick Durkin, '*Only 11 of 36 hacks revealed to market: ASIC warns on disclosure', Financial Review* (Web page, 20 February 2023) <https://www.afr.com/technology/only-11-of-36-hacks-revealed-to-market-asic-warns-on-disclosure-20230216-p5cl28>.

[42] Vilius Petkauskas, *'Mother of all breaches reveals 26 billion records: what we know so far', cybernews* (Web page, 29 January 2024) <https://cybernews.com/security/billions-passwords-credentials-leaked-mother-of-all-breaches/>.

[43] Office of the Australian Information Commissioner, *Ongoing vigilance in data protection measures essential* (Web page, 5 September 2023).

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.

What is Clyde & Co **One.**

The potential reputational damage, operational disruption and financial exposure from a cyber incident can be significant. That's why we've developed One, an end-to-end cyber risk solution, tailored to meet the needs of our clients.

We provide support whenever and wherever it is needed to restore continuity and get a client back to business as usual. We assist on all cyber and related issues, from breach readiness audits to breach response, and through to successful resolution. We can support clients with a flexible suite of services, depending on the requirements. Our 'one stop shop' offering ensures that all legal and regulatory requirements are met at every stage.

Having managed over 5,000 incidents globally, we know how to manage cyber risks.

One manages every aspect of cyber risk across the three phases:

Readiness

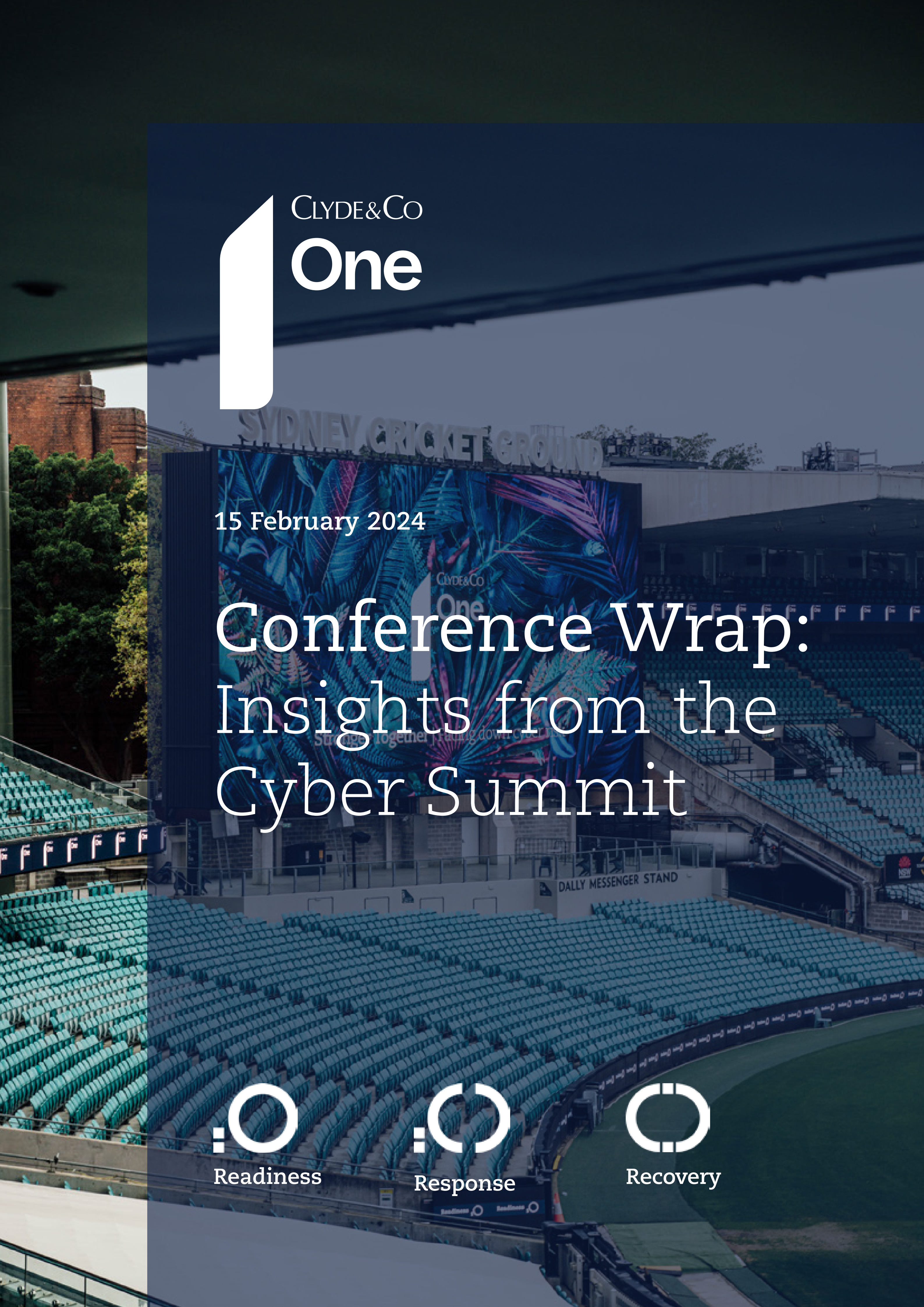
Boost your resilience and preparedness.

Response

Mitigate risk through decisive action following a cyber incident.

Recovery

Get back to business as quickly as possible.



CLYDE&CO

One

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 cyber-security 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

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.

1 ✓

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.

2 ✓

Safe technology – we can trust that our digital products and services are safe, secure and fit for purpose.

3 ✓

World-class threat sharing and blocking – we have real-time threat data, and we can block threats at scale.

4 ✓

Protected critical infrastructure – our essential services can withstand and bounce back from cyber-attacks.

5 ✓

Sovereign capabilities – we have a flourishing cyber industry with a diverse cyber workforce.

6 ✓

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.

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.

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 bought 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/content/dam/aicd/pdf/news-media/research/2024/governing-through-a-cyber-crisis-280324.pdf]

- 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

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

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.

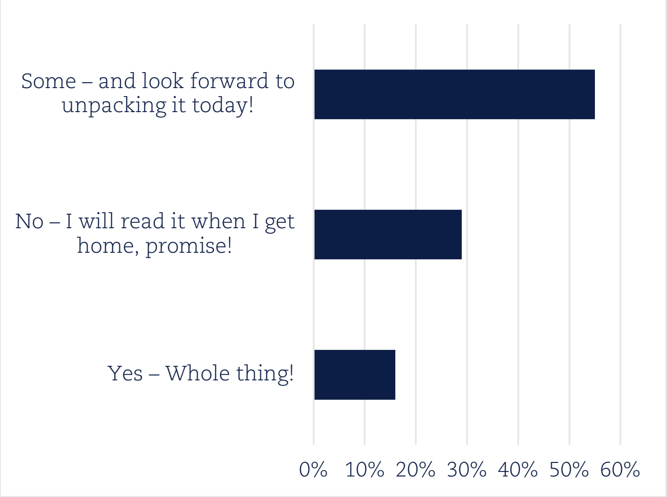
Key audience takeaways from the day

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:

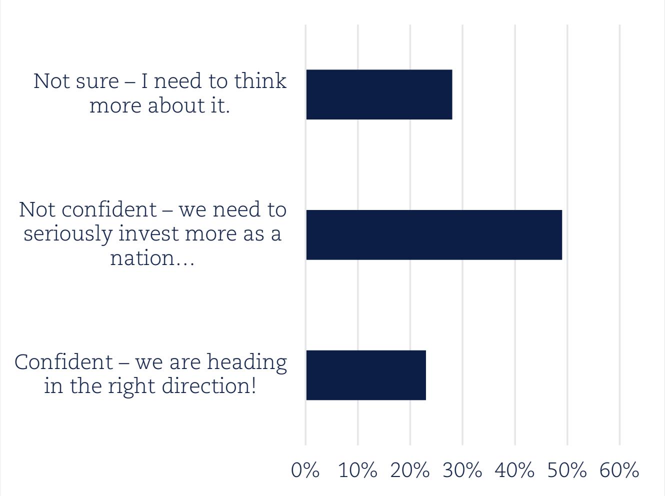
- engaging in key proposed law reforms (ransomware reporting, standalone Cybersecurity Act, SOCI);
- contributing to discussions on safe technology and threat sharing; and
- understanding our direction as a nation – our sovereign capabilities and our commitment to uplifting the region.

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?



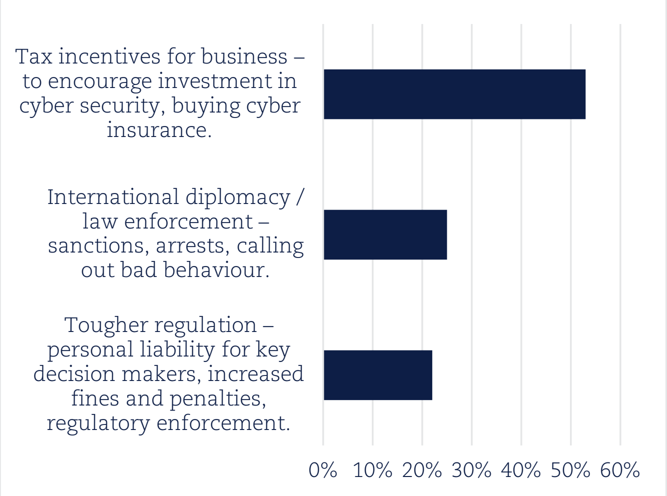
While public funding is both welcomed and anticipated, it must be met with additional resources from across the Australian economy in the form of investment in cyber readiness, response and recovery capabilities. Critically, this includes boosting the uptake of cyber insurance across the business sector (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.

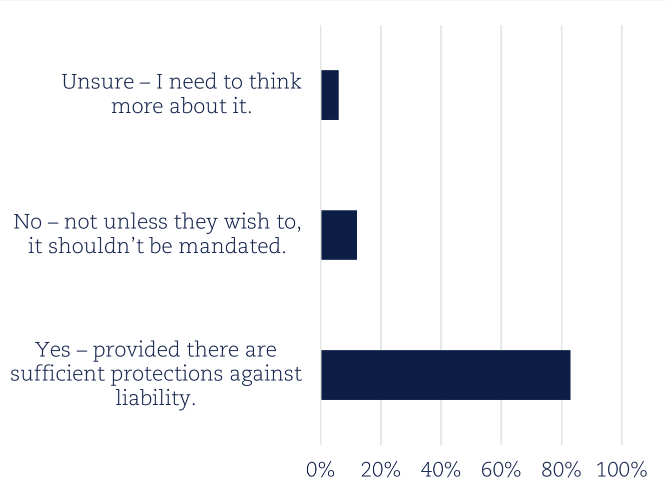
Rewarding those who are willing to invest in additional cyber resilience will encourage intentions to turn into actions, which collectively will help secure the country's IT environment as a whole.

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.

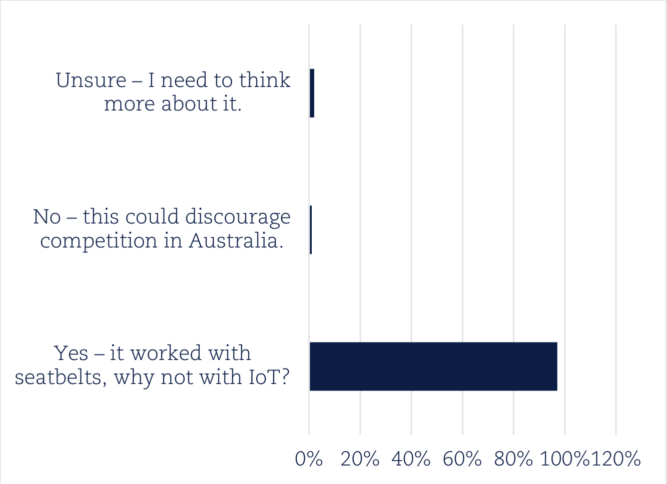
This interplay must be governed by trust, driven by information-sharing initiatives that span both the practical, and the pragmatic. As this interplay gathers pace, the opportunity will meet with the ambition – creating a valuable source of intelligence that threat actors will be unable to match.

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?

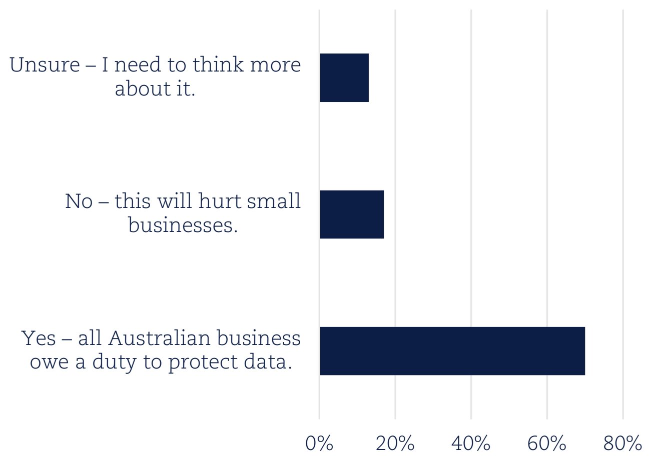


As with seat belts, imposing action may be resented by the few, but will benefit the many. The audience was strong in their support for such wholesale reform.

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?

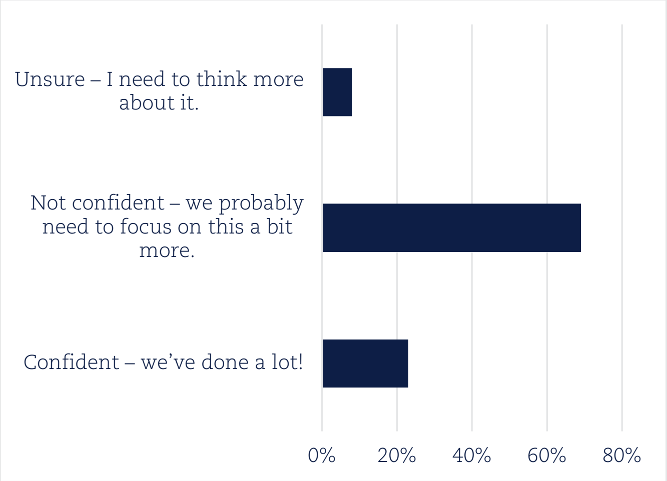


With that said, compliance with the Privacy Act comes at significant cost – the government recognises this and will be implementing various initiatives before broadening the scope of its application.

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?

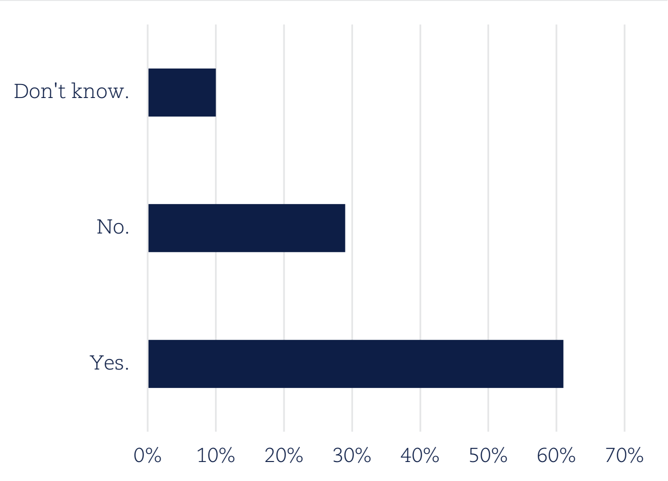


Solid rules of engagement, clear regulation and minimum security standards will provide additional confidence for organisations entering into such interactions – allowing cybersecurity to growth alongside economic opportunity.

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?

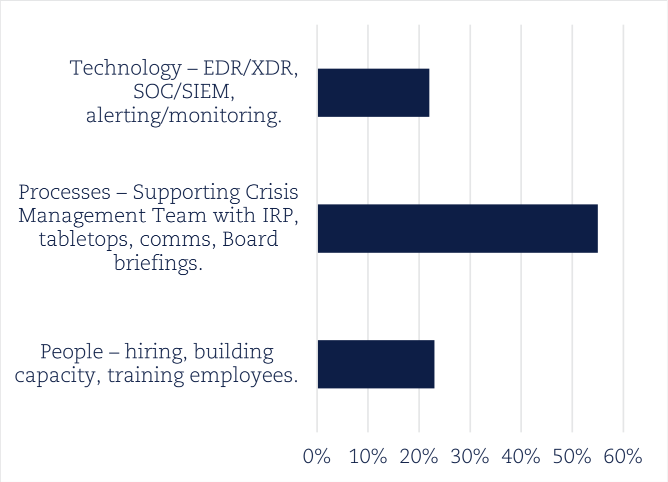


A greater investment needs to be directed towards empowering a combined response to these incidents, allowing for the additional complexity that comes from coordinating engagement and balancing the conflicting needs of different groups of stakeholders.

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 – reinvigorate 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.

- 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

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

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/

Gridware
cybersecurity
Gridwar
Containment and preservation recommendations for each compromised account.
Perform security snapsho

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 CYBER

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

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/

Triskele Labs
Follow the Sun Digital Forensic and Incident Response
Sovereign Australian Security Operations Centre
Advisory
Defensive
Offensive

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/

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

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/

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
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

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

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

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.

Key contacts

Reece Corbett-Wilkins
Partner, Sydney
[redacted]

John Moran
Partner, Sydney
[redacted]

Richard Berkahn
Partner, Sydney / Auckland
[redacted]

Stefanie Luhrs
Partner, Brisbane
[redacted]

Alec Christie
Digital Risk Partner, Sydney
[redacted]

Andrew Brewer
Director, Cyber Risk, Brisbane
[redacted]

Chris McLaughlin
Cyber Risk Advisory Principal, Sydney
[redacted]

Richard Martin
Director Communications, Cyber, Sydney
[redacted]

We also want 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