Submissions to Department of Home Affairs

IN RESPONSE TO POLICY DISCUSSION PAPER “CHARTING NEW HORIZONS: DEVELOPING HORIZON 2 OF THE 2023-2030 AUSTRALIAN CYBER SECURITY STRATEGY”

Atmos

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

By email: CSSH2@homeaffairs.gov.au

REFERENCE NO.
Horizon 2 Submission

DATE
5 September 2025

Dear Sir / Madam

Atmos' submission in response to the Australian Cyber Security Strategy 2023-2030 Horizon 2 Discussion Paper.

1. INTRODUCTION

Atmos is grateful for the opportunity to provide its insights into the evolving cyber threat landscape in support of developing legislative and policy measures aimed at strengthening Australia's resilience to cyber risk.

We commend the Australian Government for its continued commitment to addressing cyber risk at an aggregate level, and in particular the Home Affairs team who have dedicated themselves to this mission over many years.

We have focussed our submissions on the questions relating to **Shield 1: Strong businesses and citizens**. We have concentrated on how the Government can 'expand its reach' and scale its Horizon 2 efforts by partnering with the cyber insurance and incident response industry to amplify its objectives. Specifically, we have sought to identify ways that the Government can continue to scale maturity across the whole economy, by making further investments in the broader cyber ecosystem, scale up the cyber industry and grow a diverse cyber workforce.

With a particular focus on supporting micro and small businesses (revenues less than $3m, and less than $10m) and medium sized businesses (revenues $10-100m), we **recommend** that the CISG explores efforts to:

a. **Recommendation 1:** leverage the cyber insurance industry's whole of market reach to amplify resilience efforts. The industry acts as a trusted risk advisor to all organisations across every sector and in that respect is a scalable channel for distributing key messages and aligning outcomes when fully utilised. We propose the establishment of a dedicated cyber insurance working group with key stakeholders from industry and Government, such as Home Affairs, the ASD, and Cyber Wardens, to help identify and drive objectives arising out of Horizon 2. With that established, there will be further opportunities to informally identify further areas of alignment.

b. **Recommendation 2:** The Government should consider mandating, or at the very least strongly promoting, the adoption of cyber insurance solutions. Cyber insurance can serve as a strategic tool to reduce the financial impact of cybercrime across the economy and ensure that organisations have access to the necessary resources to prevent and effectively respond to cyber incidents.

c. **Recommendation 3:** establish dedicated information-sharing forums beyond existing threat intelligence sharing forums, to enable broader access to de-identified incident insights. The focus of such forums is to highlight the impact of cyber risk and benefits of cyber risk controls, underpinned by an 'all hazards' approach to addressing cyber resilience. By leading or participating in these forums, the Government can obtain useful data to further refine intervention efforts.

While our focus in this paper is on directly supporting micro, small and medium sized businesses, if implemented, the benefits will carry across to the whole of economy and all organisations within it (i.e. large and enterprise businesses, and government agencies. Even if the focus is on supporting small micro, small and medium sized businesses, the benefits, in time, will 'trickle up' through supply chains and across industries, particularly where small

businesses are contracted service providers to more highly regulated industries (such as government and critical infrastructure).

Our recommended proposals are also intended to identify opportunities to maintain continuity well beyond Horizon 2 to allow the Government to focus on continued intervention in other areas in Horizon 3, harnessing the Government's unique ability to build capacity within industry now, to drive resilience on an enduring basis. The proposals also align with the CISG's ambition to identify opportunities to intervene at an aggregate level in a scalable and efficient manner, and with maximum industry support.

We look forward to discussing these recommendations with the CISG further if there is interest.

2. ADDITIONAL MATERIALS

We have **enclosed** various supporting materials in the following Annexures:

a. **Annexure A** – About Atmos: Who we are and what we do, which underpins our perspective;

b. **Annexure B** – Insurance industry insights: identifying challenges and opportunities with promoting cyber insurance collected directly from industry; and

c. **Annexure C** – Atmos Intelligence: an example of how incident response insights and information sharing can be harnessed to lift resilience.

The views expressed in this paper are our own independent observations drawn from over 12 years of experience seeing the cyber threat landscape, regulatory environment, cyber insurance market, incident response industry and Government support evolve and shift over time.

To support our response, we have also sought the views of many within the cyber insurance industry whom we thank for their assistance with this response.[1] We also highlight that while Atmos is heavily integrated within the cyber insurance industry, we act for, and our duties are to, the entities who experience cyber incidents and it is with their interests in mind that we make these submissions. We also note that we act for various entities (small, large and government agencies) which experience incidents but don't necessarily claim on their cyber insurance policy (or don't have insurance) and so our data crosses over both insured and uninsured risks.

Our views are heavily influenced by our experience supporting on the front line, including acting for many small businesses (as well as large corporates and multi nationals) through incredibly tough times, in the battle against cyber threats, and the various perspectives across the board on where the gaps and opportunities lie.

3. OUR RECOMMENDATIONS

In our submission, we make the following recommendations to the CISG, which are focussed on identifying areas which the Government can utilise to 'expand its reach' as we move into Horizon 2.

Recommendation 1: Partner with the cyber insurance industry (insurers, brokers, and risk advisors) to amplify efforts arising out of Horizon 2

This recommendation addresses **questions 6, 7, 8 and 9** contained within the policy discussion paper.

The cyber insurance industry has dedicated itself to driving down cyber risk and building financial resilience into the economy to buffer the impact of cybercrime for nearly 30 years (and certainly in the last 5-10 years). It is an industry which is heavily invested in the protection of its clients' systems, and in ensuring that its clients can appropriately prepare for and respond to cyber incidents if their systems are impaired or data is compromised.

As a brief overview, cyber insurers protect their clients from losses and liability associated with a cyber event. This typically includes incident response costs (systems recovery, forensics, legal, data privacy, extortion, crisis

[1] We thank the following individuals for their assistance with preparing this response: Michael Joseph (Austbrokers Cyber Pro), Mark Luckin (Lockton Australia), Jennie Reed (AON), Kristine Salgado (Marsh), Pranav Jani (BMS Risk Solutions), Robyn Adcock (Gallaghers Australia) and Jodie Piddington (360 Underwriting). We also thank the numerous contributors who aren't named here, but who are passionately dedicated to making Australia a safer place to do business online and who provided useful insights for inclusion.

communications, and notification costs), third party liability exposure (defence costs, privacy liability, compensation claims and consumer redress), business interruption and downtime losses (loss of profits and reputational harm), misdirected funds from social engineering (funds transfer fraud), the costs of responding to supply chain attacks involving personal information jointly held by third party processors (i.e. multi-party data breaches), and fines and penalties associated with regulatory investigations (and associated investigation costs).

Depending on the specific needs of an organisation, cyber insurance can also cover property damage losses caused by cyber incidents (particularly relevant for critical infrastructure operators), contingent business interruption losses for downtime of key suppliers (responding to recent network outage events in 2024), as well as various affirmative covers applicable to certain organisations/industries. These covers are more relevant to manufacturing entities which aren't heavy collectors of personal information but are more concerned with operational integrity and business continuity impacts if their systems go down.

For small businesses, the average self-reported cost of cybercrime is $49,600[2] (our own data shows the costs are more than this), with the average costs of cybercrime to the Australian economy being $42 billion a year.[3] Obviously this latter figure covers a broad range of directed and indirect losses on an accumulated basis across the wider economy, including to individuals.

However, within the business sector, we estimate the direct and indirect costs to organisations would easily be in the billions of dollars every year, with the potential for losses to be much greater as threat actors become more destructive in their activities. The domestic cyber insurance market sits at a comparatively modest $650 million in Gross Written Premium (GWP), which is significantly less than the actual and potential financial exposure to the economy.[4] There is a real issue with organisations being both uninsured, and underinsured (even where they do hold cyber insurance).

To date, the cyber insurance industry has been **underutilised** as a mechanism to amplify cyber security uplift efforts across the whole of the economy and particularly the small business sector. Its true value is only available to the relatively small percentage of organisations that purchase cyber insurance, who can access the pre- and post-loss service offerings, education, and resources that accompany the insurance product to prevent cyber incidents in the first place and protect against losses should they occur.

Most importantly for small businesses it provides a level of enhanced response capability that is unachievable without insurance. This is not only important for the business to be able to rebound, but also to consumers and individuals whose information is compromised. Those individuals deserve the support that only large and enterprise businesses can realistically afford.

From the perspective of an individual involved in a data breach, it makes no difference to them if their local conveyancer or real estate agency (small business), or their bank (large corporate), suffers a data breach involving their 100 points of ID. They require the same level of support either way to protect against data misuse risk and support them through their remediation and response journey. This is particularly so with the rising concerns of the 'mosaic effect' of multiple data breaches occurring across the nation and the combination of datapoints involved per individual.[5]

However, while a bank will have seemingly unlimited resources to 'right the wrong', investigate the breach, assess the data impact, notify individuals and take whatever steps are necessary to protect them – small businesses simply do not have this resource capacity or financial war chest to do this. The sheer reality is that without insurance, small businesses will focus on doing whatever they can within their means and often that means making sacrifices.

That's not to say small businesses don't care. To the contrary, we've acted for small businesses who have gone **far above and beyond** what's reasonable (we have countless stories, but one example that sticks out was a small MSP business owner that re-mortgaged his house to pay for the costs of restoring his client's data on the back of a ransomware incident). It's simply to say that there are limitations on what's realistically achievable for small

[2] https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024.
[3] https://www.unsw.edu.au/news/2021/12/cybercrime-an-estimated--42-billion-cost-to-australian-economy.
[4] https://a.storyblok.com/f/132489/x/053e374555/finity-optimalite-2024.pdf.
[5] https://www.abc.net.au/news/2023-03-28/detailed-portrait-data-breaches-oaic-disclosures/102131586.

businesses, without insurance.

While the incident response industry (including Atmos) dedicates significant pro-bono hours to support small businesses and individuals caught up in cybercrime each year – there is only so much we can do. Instead, a big focus over the last three years has been working with the market to develop hyper cost-effective incident response solutions for small business to drive costs down with a focus on proportionality. Again, there are limitations here too, particularly for large scale incidents that involve small businesses (such as ransomware).

The opportunity to profile and partner with the cyber insurance industry is easily within reach. For example, if you search the 2020 and 2023 cyber strategies, there are zero references to 'cyber insurance'[6] – although the industry did receive one mention in the 2016 strategy,[7] which way back then recognised the '*rapidly growing cyber insurance market*' and its potential to '*help enforce improved cyber security performance*'.

The CISG has the opportunity in Horizon 2 to publicly acknowledge the contributions of the cyber insurance industry and identify areas to collaborate more effectively to achieve common objectives at scale, harnessing the cyber insurance industry's whole of market reach to amplify key messaging (particularly supporting small businesses).

To demonstrate the opportunity, over the past 10 years, the cyber insurance industry has been quietly helping tens of thousands of organisations improve their cyber security controls at scale and continues to invest heavily in promoting further preventative controls as the threat landscape evolves. Some insurers have positioned their products around being a '*promise to protect*', as well as being a '*promise to respond*' and a '*promise to pay*', with various add on features available to achieve this. Some insurers are providing protective services (at their own expense, or subsidised) to protect their clients' assets and prevent breaches altogether.[8] This includes real time threat and alert monitoring, and advisory services to help clients improve their posture once a policy is bound.

While each insurer's approach and appetite for risk differs slightly, broadly speaking the industry has identified the most effective minimum-security controls to drive an organisation's cyber resilience (such as driving the push to implement MFA on core systems and regular patching of critical vulnerabilities) and thereby prevent low-hanging fruit breaches. Enforcing call back procedures to limit the instances of social engineering fraud on the back of business email compromise events is another example.

In short, once a business obtains cyber insurance, their risk becomes the insurer's risk. The onus shifts on the insurer to drive down the frequency and severity of attacks to protect their own financial exposure, thereby creating a force mechanism to enhance resilience efforts at scale. Through enhanced underwriting requirements, these controls are typically mandated across policyholders' environments, with various support mechanisms available to implement control enhancements pre-bind or within a certain timeframe post-bind (i.e. within 30 days of policy inception). These efforts align with the Government's broader mission to increase awareness about cyber security risks more generally, and drive action to prevent and minimise the impact of common attacks across the economy.

For smaller businesses, this '*insurability*' process allows organisations to become more 'cyber secure' while also purchasing cyber insurance capital to scale their response capabilities and protect their bottom line. It also reduces the competition for finite resources, particularly when organisations weigh up between 'investing in cyber security' or 'investing in cyber insurance'.

Various insurers are aligning with the MSP/TSP industry to demonstrate how to achieve both in a cost-efficient way, at the same time, with the same or similar budget. Many MSPs/TSPs have also recognised the opportunity for insurers and brokers to support them in their efforts to better educate their clients on the need for enhanced controls. While there is still a long way to go to build bridges and demystify misconceptions, there is a natural synergy between what MSPs, insurers, and Government are trying to achieve, by working better together.

As an aside, having supported various many MSPs/TSPs with incidents (some large, some small) – what is emerging

[6] https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf, and https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf.
[7] https://www.homeaffairs.gov.au/cyber-security-subsite/files/PMC-Cyber-Strategy.pdf.
[8] https://www.chubb.com/content/dam/chubb-sites/chubb-com/us-en/business-insurance/products/cyber/documents/chubb_cyber_stack_final.pdf; and https://www.cfc.com/en-au/knowledge/resources/articles/2025/03/cyber-product-enhancements-proactive-services/. We note that these are two of many insurers which offer similar services.

is that some are now hesitant to take on clients unless they have their own cyber insurance. This is to try and derisk their own liability exposure should an incident arise and ensure that there is sufficient incident response support should the MSP/TSP be capacity constrained to assist their own client(s) during an incident. This trend is also reflective of the MSP/TSP industry's role in explaining to clients that just because security has been outsourced to a third party, the responsibility still rests with the client. There's also a need for MSP/TSPs to better articulate that there are always risks of cyber-attacks even if MSP/TSP are engaged to provide managed services.

For larger organisations, 'insurability' mapped against recognised industry best practice sends a clear message to the Board and decision makers: you need to have certain controls in place before you're considered to be a good risk in line with certain industry standards. Insurability as a benchmarking tool for good cybersecurity is a useful guide for Boards to assess their adequacy of their cyber security posture and understand from insurers where to focus their efforts based on industry insights relevant to their organisation.

In the same way that certifications (SMB1001, ISO27001, SOC2, Essential Eight, NIST CSF, etc) can be a useful way to enforce minimum cyber control standards, so too is insurability. Insurability gives confidence to the market that the organisation has been vetted against industry benchmarks and in turn, gives that organisation confidence to focus to go to market. This is particularly so if the organisation operates within highly regulated supply chains, where strong cyber security control maturity (and in many cases, cyber insurance) is a prerequisite to winning contracts.

In this way, insurability and being adequately insured against cyber risks can help drive market confidence. It will contribute to increased productivity measures and unlock competition for smaller players to compete in the market, which is a key feature on the Government's agenda at present. Finding ways to reduce barriers to entry for small businesses should be explored.

When harnessed to its full potential, organisations can also leverage insurers' local and global insights into cyber risks including accessing 'warning signals' for key attack trends and campaigns that may be coming down the line. Organisations are starting to tap into this resource pool, acknowledging that the cyber insurance industry is a global industry, which sees attack trends and liability exposure factors even before they hit the Australian market. For example, when a trend is observed in the US, it often spreads to Australia within 1-3 months. The recent Akira / SonicWall campaign is a good example of this.

Taking all the above into account, we commend the Home Affairs team for their significant investment of time and effort in developing relationships across the cyber insurance and incident response industries over the past few years, including hosting various industry roundtables, attending industry conferences, and hosting various discussion groups with this sector.

However more can be done to harness this resource further, as we move to scale.

We recommend that CISG considers:

a. *The establishment of a dedicated cyber insurance working group with key stakeholders from industry and Government, such as Home Affairs, the ASD, and Cyber Wardens, to help identify and drive objectives arising out of Horizon 2. This includes ways to leverage the vast resources available through the cyber insurance industry more broadly to scale education, awareness, and specific interventions necessary to drive down cybercrime across the economy (particularly for small businesses and certain industry sectors where the impact of cyber risk is greatest).*

Recommendation 2: Mandate or heavily promote cyber insurance for small businesses and certain industries where cyber risk consequences are highest.

This recommendation addresses **questions 5-11** contained within the policy discussion paper.

We openly acknowledge that the Government is not in the business of selling cyber insurance policies and cannot promote a particular product. We also acknowledge that in setting the Horizon 2 strategy, the Government will need to carefully approach how it supports public policy development alongside any existing private sector solutions available to the market, without promoting a particular industry, product or service.

However, as a matter of public policy, we recommend that the CISG considers:

a. ***Option 1:*** *to reach the masses, mandating the uptake of cyber insurance across all micro and small businesses (say with revenues of less than $10m). Alternatively, mandating cyber insurance across certain parts of the economy such as for small businesses or for industries where cyber risk consequences are highest. This has been implemented in other areas such as compulsory third-party motor vehicle insurance, or workers compensation insurance for employees, recognising the need for broad economic protection to protect the community.*

b. ***Option 2:*** *Introduce a requirement for all Government service providers to hold cyber insurance as part of contracting arrangements. This would signal the Government's implicit endorsement of the need for cyber insurance. It also aligns with the Government's broader position that all federal, state, and local agencies should maintain cyber insurance coverage, whether through commercial policies, self-insurance arrangements, or mutual schemes.*

c. ***Option 3:*** *recognising that Options 1 and 2 will likely require further policy assessment, in the meantime, and as a minimum, heavily promoting cyber insurance across the economy, or for industries where cyber risk consequences are highest. For example, aggregation industries such as managed service providers (MSPs), technology service providers (TSPs), professional services handling sensitive data, health service providers, and financial institutions. This could be as simple as baking 'cyber insurance' consistently into all resilience advisories promoting best practice. This is a model that the WA Government has already implemented in its cyber security policy framework.[9] Or it could be a government led campaign to better educate and promote the benefits of cyber insurance across the economy and delivered through existing solutions such as the 'CyberWardens' program which has a reach into small businesses. 'CyberWardens' could easily partner with the insurance industry to develop a module on the benefits of cyber insurance.*

d. ***Option 4:*** *If the Government is unable to commit to these proposals as part of the Horizon 2 strategy, we recommend that the CISG considers commissioning a report to understand the benefits and costs associated with enforcing a mandatory scheme, working alongside the insurance industry, the Insurance Council of Australia, the Australian Institute of Company Directors, and other industry peak bodies such as COSBOA, BCA, ANZIIF, NIBA etc. This would enable the Government to better identify the level of targeted intervention that is reasonably necessary to achieve scale.*

The requirement to obtain insurance as a pre-requisite for doing business isn't novel. The private market already mandates this in certain highly regulated sectors, including in supplier due diligence and pass through obligations in supplier contracting requirements.

However, often the requirement is limited to obtaining professional indemnity and other liability insurance and does not specifically contemplate cyber insurance despite the various privacy, security, liability and other related contractual clauses typical in commercial contacts. These clauses often set high standards of care when it comes to the protection of data, systems and cyber response protocols without any appreciation for the contracting party's ability to comply (particularly small businesses).

Even where cyber insurance is contractually imposed by more mature entities to their suppliers (typically highly regulated industries), leaving it to the private market to address this is not scalable on a 1:1 basis, unless it were mandatory in all contracts.

Leaving parties to privately negotiate supplier terms also lacks uniformity and clarity in terms of the types of insurance required (i.e. noting the vast differences between a cyber liability product vs a standalone cyber insurance product) and the levels of cover required to adequately cover risks (i.e. $1m limits vs $5m vs $10m+ limits). This results in patchy uptake, and often supply chains are left with inadequate protections overall, even where cyber insurance appears to feature as a contractual requirement.

As above, we've proposed that empowering small businesses to purchase cyber insurance this could unlock productivity and increase competition in the market, allowing small businesses to compete with larger enterprises and provide market confidence. The obvious counterargument is that by mandating cyber insurance it could in the short-term risk stifling commerce by creating too high a barrier to entry. However, as insurance uptake increases, we

[9] https://www.wa.gov.au/system/files/2024-12/wacybersecuritypolicy.pdf.

would expect entry level premiums to become lower and is unlikely to present a significant barrier in the medium to long term. The cyber insurance market is already positioned now to offer incredibly competitive pricing terms.

To give context to why this is a necessary intervention from the Government as part of Horizon 2 scaling initiatives, at present, estimates of insurance penetration vary with some estimates as low as 5-20% for small businesses.[10] Anecdotally, this number is likely to be even lower for micro businesses, and businesses in regional and remote areas outside of capital cities, where support for cyber response is likely to be even more limited.

Given the frequency and severity of attacks for small businesses, and the regulatory landscape which a lot of small businesses operate in, the penetration rate for cyber insurance should be much higher (in line with the 70% penetration amongst larger enterprises). There is no rational reason why small businesses aren't buying cyber insurance as often as larger enterprises.

Waiting for the small business exemption to be abolished in the Privacy Act to drive this across micro businesses, isn't the solution and in any event wouldn't necessarily lead to higher adoption rates. Given the current 'productivity vs regulation' debate on foot, it is unclear whether the Tranche 2 privacy reforms will proceed in the near term.

That said, we anticipate that such regulatory reform would drive insurance uptake (we saw this when mandatory reporting came online in 2018 under the Notifiable Data Breaches Scheme, GDPR, and in other mandatory breach reporting regimes across State and Territories and within certain industries since) as organisations recognised the value in being able to confidently respond to data breaches.

Another benefit of cyber insurance is ensuring business in run-off can afford to deal with incidents notwithstanding their capital constraints. Events such as Medisecure, highlight that various organisations often do not have sufficient capital to deal with large scale incidents. This is particularly so if they enter voluntary administration/liquidation, leaving the Government and industry to pick up the costs (and leaving affected individuals whose data is breached unsupported).

The OAIC has publicly commented on this, stating at the time:

> *At this stage, the OAIC will not pursue an investigation into the personal information handling practices of MediSecure as the possible remedies that we could obtain for the community will not be proportionate to the resources required for a comprehensive investigation. This should not be of comfort to any organisations that hold personal information and do not have appropriate data security policies and practices in place. It demonstrates that organisations need to make protecting individuals' personal information a top priority, as a data breach may destroy an organisation's reputation and cause enormous damage to the community.*[11]

Many in the incident response industry agree that more should be done to compensate for the possibility of high-risk data breach events for end-of-life companies. Insurance is one of the compensating controls to mitigate this possibility.

Something that's not talked enough about are the thousands of examples every year where organisations have been able to adequately respond to cyber incidents with the full support of the insurance policy sitting behind them. When comparing the breach response efforts of small businesses, it is often obvious which have cyber insurance and can properly respond and those which don't. More should be done to showcase what good looks like and explore why.

The question then is why cyber insurance penetration rates are so low (particularly for small businesses). Historically, cyber insurance has been seen as being too expensive, or difficult to acquire. However, the price of cyber insurance has significantly reduced due to the competition in the market and excess capital that the insurance industry has available to invest in underwriting cyber losses. Further, the breadth of coverage is wider than it's ever been before, and the barriers to entry are much lower.[12]

[10] https://insurancecouncil.com.au/campaigns/defend-critical-infrastructure/cyber-risk/; https://www.reinsurancene.ws/cyber-insurance-premiums-stabilise-in-2025-but-market-penetration-remains-below-10-for-smes-sp/.
[11] https://www.oaic.gov.au/news/media-centre/statement-on-medisecure-data-breach-september-2024.
[12] https://www.swissre.com/risk-knowledge/advancing-societal-benefits-digitalisation/cyber-insurance-growth-shift.html.

Unfortunately, these messages are not reaching the business community at scale (particularly small businesses). This results in non-cyber insurance brokers spending significant time demystifying the benefits of the value of cyber insurance to an audience who themselves are ill-equipped to fully understand the risks that they face. Too often we see small businesses impacted by a cyber incident say, *'if only I knew what cyber insurance would have covered, I would have purchased it'*. Unfortunately, there is not enough broad scale support from outside the insurance industry to amplify the benefits of cyber insurance, which is a major reason why it is an underutilised asset.

To assist the CISG in understanding the challenges with the promotion of cyber insurance, we have set out various responses from the industry in **Annexure B**. It is hoped that these insights provide useful context for the opportunity in front of the CISG in considering this issue further.

While brokers are trusted risk advisors to all businesses (particularly small businesses), one major challenge is continuously upskilling the 15,000+ general insurance brokers across the country on how to have informed and relevant conversations about cyber risk, cyber controls, and cyber insurance. Many fear not being able to hold a credible conversation with clients, particularly with the rapidly evolving landscape, and therefore the opportunity to build cyber resilience is lost.

While the industry is doing all that it can to educate themselves (including dedicated certification courses[13] and insurer led courses[14]) it is a highly inefficient way to drive scalable outcomes. That said, we acknowledge the immense efforts of various leaders within the cyber insurance industry who have done a lot to raise the baseline of education, for the benefit of clients and the protection of our economy.

This is where Government endorsement or programs such as '*CyberWardens*' could assist, by bringing both cyber security and cyber insurance into the same conversation. Anecdotally, we hear from brokers that it takes 3+ years of talking about cyber insurance before a client is interested in considering purchasing. In other words, even where brokers are actively engaging on the topic, the need from clients is not well-understood and the conversation is therefore overshadowed by costs, if it even gets to that point.

There is an opportunity with Horizon 2 to better promote the benefits of cyber insurance (as set out our in our recommendations above) particularly to those sectors who are unable to respond to incidents properly without the benefit of cyber insurance. This will drive more small businesses to 'ask their broker' for more information about the benefits of cyber insurance, rather than the other way around, if they are prompted to do so from sources outside of the industry.

In some ways, it is no different to the ASD's initiative way back in 2017 to upskill businesses on questions to ask their MSP to better inform both sides of the bargain.[15] Fundamentally, the root cause issue remains: how to upskill the small business sector on better understanding their risk, to allow them to better understand and control their situation.

Recommendation 3: Identify areas for sharing experiences beyond the existing threat intel sharing frameworks.

This recommendation addresses **questions 5, 12, 13 and 14** contained within the policy discussion paper.

Various players within the breach response ecosystem are data aggregators and hold a wealth of incident related data which can be harnessed to share insights, develop policy, encourage targeted investment, prevent further attacks, and increase reliance.

DFIR firms, law firms, insurers, brokers, threat intelligence firms, negotiators, and MSPs all hold the keys to this data, but being able to unlock these insights in a digestible way is where the challenge and the opportunity lies. There are examples however where this information is available, such as the annual NetDiligence Cyber Claims Study, which presents the US cyber claims market data from various market participants.[16] While not perfectly comparable to the Australian market (given the size of the US market), it is a good indication of what can be done from an information

[13] https://www.cyberinsuranceacademy.com/.
[14] https://www.cfc.com/en-au/cfc-cyber-masterclass/.
[15] https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/outsourcing-and-procurement/managed-services.
[16] https://netdiligence.com/wp-content/uploads/2025/04/NetDiligence-Cyber-Claims-Study-2024-Report-V1.1.pdf.

sharing perspective.

Often this data may be commercially sensitive, or considered intellectual property, and may not be sharable. Further, without there being a net benefit for the collection, classification, and presentation of this data, there is little commercial imperative for this information to be shared. That said, everyone in the industry agrees that it is possible, with the right support frameworks in place.

To assist the CISG in understanding what de-identified information sharing could look like, we have enclosed at **Annexure C** our latest 'Atmos Intelligence Insights Series' advisory, which we have delivered to the cyber insurance market in Australia, New Zealand and the UK across August 2025. This advisory not only shines a light on the cyber threat landscape trends over the last quarter but also calls out various areas where further efforts are required (and which industry sectors and business sizes require maximum support).

We acknowledge the Government's focus on developing real-time threat sharing and blocking which for obvious reasons, is a very worthwhile pursuit to intervene at the 'top of the funnel' to stop or slow down attacks. The efforts of Government and industry to embark on efforts such as "Cleaner Pipes" are a great example of disrupting criminal enterprise at the source.[17]

While these efforts are incredibly commendable and should continue, they don't '*tell the story*' and allow small business owners and key decision makers to learn from others in this space on issues relevant to them. Developing industry specific advisory networks with a focus on certain areas (such as the NFP sector as one example) should be considered.

The Government is to be commended for its efforts in bringing together sector specific initiatives (such as the playbooks developed by the National Office of Cyber Security) and the Trusted Information Sharing Network (TISN) for critical infrastructure operators.

However, the same opportunities don't exist for small or mid-market businesses. Partnering with industry peak bodies and the incident response industry to deliver lessons learned is an efficient way to reach maximum audience with minimal capital or time commitment. While confidentiality and legal professional privilege are always factors that prevent information sharing, there are opportunities to share this information on a de-identified basis within appropriate information sharing controls in place.

More broadly, the incident response industry has become accustomed to managing large scale data breaches. While they are difficult to deal with, we are heading in the right direction with efforts to reduce the impact of breaches. One example includes the recent introduction of the Compromised Credential Register in NSW, which will in time significantly reduce the number of wallet IDs that need to be replaced in the wake of a major ID theft incident, and stop or slow down the ability for identity theft to occur.

What we are all really worried about within the incident response industry is the ability to respond to a major cyber incident which causes loss of life or livelihood, off the back of a wide scale, or enduring incident with real world impact. This is something that the National Office of Cyber Security is alive to, and significant resilience efforts are underway to prepare for this possibility.

By amplifying the foundations developed over the past three years, the CISG can implement strategies to strengthen industry resilience around cyber risk. By adopting an 'all hazards' approach, the conversation can move from purely cyber risk prevention, to 'all hazard' harm prevention, through controlled information sharing forums.

This includes working proactively with aggregators which, if impacted by an outage, or a multi-party data breach, can cause significant downstream impact for organisations and individuals alike. Real world examples include incidents involving common service providers / technology service providers (such as the 2024 EDR provider outage) or specific industries where real world financial, economic and social harm is more likely (such as critical infrastructure organisations with a focus on delivering health, financial, energy, transport and logistics, and frontline support).

The Government is to be commended for spearheading industry led tabletops and cross-sectoral resilience

[17] https://www.telstra.com.au/exchange/safer-online-and-the-new-normal.

initiatives across certain sectors already, with further works to continue to bolster these industries and their supply chains.

We recommend that CISG considers:

a. *The establishment of a dedicated information sharing forums for certain industries beyond the existing threat intel frameworks. This can be aligned within existing intel sharing frameworks harnessing existing information sharing controls, with a particular focus on industry sectors that cannot obtain these insights.*

4. WHERE TO FROM HERE

We are happy to expand on the above recommendations should the CISG require further information, particularly in relation to **questions 12-14** (which focus on ransomware threats and how to prevent them).

Please let us know if you require any further information from us in the interim.

Yours sincerely

ANNEXURE A - ABOUT ATMOS: WHO WE ARE WE AND WHAT WE DO

Atmos is a specialist legal and advisory firm providing a wide range of services with an exclusive focus on cyber, privacy and digital risk across Australia and New Zealand.

We recently launched in early 2025 and have a team of 65+ team members situated across Australia and New Zealand. We're committed to supporting our region navigate the complexities of this space and will continue to invest heavily in our growing capability to do so.

Using our combined experience managing thousands of incidents consistently over 12+ years, we have a unique understanding of the factors contributing to the frequency and severity of cyber events for small, mid-market, and enterprise businesses and government agencies.

We work in partnership with our clients and the industry to address risk factors in advance of an incident and build resilience throughout their operations. We safeguard when things go wrong and are there to address the long-tail exposures of cyber, privacy and digital risk.

It is this cross-discipline experience which allows us to focus on the following areas, which we have built specialty teams around:

a. Readiness: pre-breach resilience;

b. Response: 24/7 incident response;

c. Recovery: post-breach remediation;

d. Disputes + Investigations: claims defence and regulatory investigations;

e. Directors + Officers: education and awareness, and personal liability defence; and

f. Crisis Communications: non-legal crisis comms.

Our 'First Response' service offering is the bedrock of our firm's capabilities, and through the team we act as 'incident response managers' or 'breach coach' for entities that experience a cyber, privacy or digital risk incident. 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, to support our response efforts, which is where our in-house 'Atmos Intelligence' is sourced (see **Annexure C**).

More broadly, our legal, regulatory, and crisis management expertise allow us to be trusted advisors across all industry sectors, deploying our in-depth capability and capacity to service incidents both large and small. We partner closely with industry experts across multiple domains including the broader incident response sector.

We are powered by the cyber insurance industry, corporate and government clients, and broader industry in the mission to face down cyber risk. We also work closely with government agencies (such as the ACSC, NOCS and law enforcement) to drive various initiatives and have strong relationships across the sector.

We have contributed heavily to the development of public policy and legislative frameworks around cyber risk efforts including providing submissions to all major discussion papers,[18] attending webinars and Q&A sessions, participating in round tables, giving evidence to parliamentary inquiries,[19] and hosting various events (including major cyber conferences) evangelising the Government's efforts to uplift the whole of nation cyber security.

It is with pleasure that we can continue to contribute to these efforts through this submission and look forward to seeing the development of Horizon 2 of the Cyber Security Strategy.

[18] If possible, the CISG should search its archives for a copy of our 2020 cyber security strategy submissions to the then Minister for Home Affairs, Peter Dutton, which contains a wealth of historical data in relation to cyber attack trends and insurance trends. Unfortunately, it was submitted on a confidential basis and we no longer hold a copy, but a lot of the content we prepared for those submissions are still relevant today.

[19] https://www.aph.gov.au/Parliamentary_Business/Hansard/Hansard_Display?bid=committees/commjnt/27957/&sid=0001.

ANNEXURE B - INSURANCE INDUSTRY INSIGHTS: IDENTIFYING CHALLENGES AND OPPORTUNITIES WITH PROMOTING CYBER INSURANCE

The role of insurance in the cyber industry

Cybercrime is costing the Australian economy an estimated $42 billion a year,[20] while the domestic cyber insurance market sits at a comparatively modest $650 million in Gross Written Premium (GWP)[21]. These figures are worlds apart and highlight a critical opportunity. Why allow cybercriminals to extract billions from our economy when the insurance industry is ready and willing to mitigate that risk?

Cyber insurance is more than a financial safety net; it is a strategic tool that actively contributes to Australia's cyber resilience. As the Government seeks to expand its reach and uplift cyber maturity across the economy, the insurance industry offers a powerful, underutilised lever to support this ambition.

While the process of obtaining cyber insurance can be extensive, it brings significant benefits. Insurers require organisations to implement security controls that often align with government standards, meaning businesses are adopting best practices simply through the act of seeking coverage. This alignment creates a natural synergy between public policy and private sector capability, helping to raise the baseline of cyber maturity across industries.

Insurers and brokers also play an educational role. With deep expertise in cyber risk, they help organisations understand risks and implement effective mitigation strategies. Brokers, in particular, act as trusted advisers, amplifying key messages and promoting cyber literacy across the market. This influence is especially important as insurers increasingly integrate proactive technologies; such as vulnerability scanning, dark web monitoring, and credential exposure remediation into their offerings, helping reduce the frequency and severity of incidents.

Despite these benefits, cyber insurance uptake remains low, particularly among small and medium-sized businesses. This gap presents a significant risk, as small and medium-sized businesses are often the least equipped to respond to cyber incidents and the most vulnerable to their impacts.

We have seen firsthand the consequences for uninsured or underinsured businesses, ranging from financial distress to an instance of a complete business shutdown. Regulators and consumers increasingly expect timely and proportionate responses to cyber incidents, and lack of insurance is not considered a valid excuse for inadequate action. This places uninsured organisations at a disadvantage, often resulting in gaps in response quality and speed.

Importantly, cyber insurance does pay. Contrary to headlines suggesting otherwise, declinature rates are extremely low, just a handful of cases among thousands. Coverage is intentionally broad, and when disputes arise, they typically stem from misaligned expectations rather than policy failure. Standalone cyber policies remain the most reliable form of protection, especially for first party costs and business interruption losses.

To truly expand its reach, the Government should consider working with industry leaders to mandate cyber insurance for high-risk sectors, similar to how other forms of insurance are required in regulated industries. This would not only protect critical infrastructure but also drive uplift in cyber hygiene across the board.

To support the Government's strategy, there is a clear opportunity to promote cyber insurance as a key enabler of effective incident response and broader cyber resilience. This includes targeted support for SMEs, who often lack the resources to navigate complex security controls. By integrating cyber insurance into the national strategy, the Government can help bridge the gap between risk and readiness, ensuring that organisations of all sizes are equipped to respond to and recover from cyber threats.

The challenges in 'selling cyber insurance'

To better understand the challenges surrounding cyber insurance adoption, we engaged with a broad network of brokers and insurers across the industry. Our objective was to identify the key barriers to uptake and explore how Government could play a more active role in supporting broader adoption across sectors. To guide this engagement, we posed the following question:

[20] https://www.unsw.edu.au/news/2021/12/cybercrime-an-estimated--42-billion-cost-to-australian-economy.
[21] https://a.storyblok.com/f/132489/x/053e374555/finity-optimalite-2024.pdf.

> *Given that cyber insurance penetration remains lower than expected, what do you see as the key challenges in selling cyber insurance or customers buying it? What factors contribute to these challenges, and what would you like to see from Government in terms of recognising its benefits and supporting broader adoption?*

The full responses are provided below, but the key themes raised by industry participants can be summarised as follows:

a. **Low uptake among small businesses:** small businesses remain uninsured and underinsured due to limited resources and lack of cyber expertise around their exposure.

b. **Lack of awareness and understanding**: small businesses often lack awareness of the benefits of cyber insurance, but uptake rises sharply when its value is clearly explained.

c. **Perceived lack of value**: There is a common perception that cyber insurance does not offer value for money. This is compounded by misconceptions, often amplified in media reporting, that insurers do not pay out on cyber claims.

d. **Complexity of cyber risk**: The nature of cyber threats evolves rapidly, making risk hard to define and undermining confidence in cyber insurance.

e. **Premium volatility**: Historical fluctuations in cyber insurance premiums have discouraged adoption. Although pricing has stabilised in recent years, uptake has not yet recovered accordingly.

f. **Recognition of cyber insurance in national strategy**: Government can boost national cyber resilience by recognising insurers as strategic partners, not just financial backstops.

g. **Targeted support for small to medium sized businesses**: Cost-effective, tailored solutions, backed by government incentives, can help close the protection gap for small and medium-sized businesses.

h. **Facilitating data sharing**: Brokers and insurers hold rich cyber risk data, government partnerships could unlock it to inform policy and improve modelling.

Response from an Australian based specialist cyber insurance brokerage

From my perspective I think cyber insurance is affordable for SME businesses but the problem to me and why the uptake in cyber insurance is still not where it should be really comes down to a lack of education as to how valuable the product is, and I think it really comes down to brokers still not really being educated on the product and explaining the benefits correctly to clients.

Without going into a heap of detail, when we engage with a client and explain the benefits including the proactive incident response and assistance a client gets at the time of an incident…when a client truly understands the tangible benefits of the policy, we see the take up rate in excess of 80% so I really think non-specialty cyber brokers need to spend more time on educating themselves around the product so they can educate their clients, or of course, outsource it to a specialist cyber broker.

Response from a global insurance brokerage firm

Executive Overview
The key challenges in cyber insurance adoption stem from misconceptions ("cyber insurance doesn't pay"), confusion with traditional insurance products, and the false dichotomy of investing in cyber security versus insurance. These are compounded by affordability concerns for SMEs and limited awareness of the insurer's role as a "proxy regulator" setting baseline security standards.

In practice (as further elaborated by insurer loss ratios and statistics), well-structured cyber insurance policies do pay, and insurers are paying billions globally each year, while also providing quantifiable security insights and incident response benefits. For customers, the issue is often understanding scope, navigating minimum security standards, and reconciling budget trade-offs.

Government can support broader adoption by:

- *Publicly recognising insurance as a critical enabler of resilience, not just a post-loss product.*
- *Educating SMEs/NFPs on affordability, accessibility, and the complementary role of cyber insurance alongside controls.*
- *Mandating inclusion of insurers in threat-sharing frameworks, highlighting their unique claims-driven insights.*
- *Considering incentives or safe harbours for organisations that hold cyber insurance and meet maturity benchmarks.*

Background of the Australian Cyber Insurance Market

GWP
The Australian cyber insurance market has experienced remarkable growth:

- *From approximately AUD 500m in FY23 to around AUD 650m in FY24, representing a growth rate of around 30% year-on-year (2024 Optima Lite – General Insurance Insights – Finity.)*
- *Forecasted to grow steadily at around 20% annually over the next two to three years, driven by increased demand, heightened awareness post-significant breaches (e.g., Optus, Medibank), and continued regulatory focus (Privacy Act reforms).*

Penetration

- *A survey of the ASX200 (in 2022 by Macquarie Research (Australian General Insurance Battlefront: Cyber FY22)) found ~68% purchase Cyber Insurance. The Insurance Council of Australia have also noted significant underinsurance in Australia for cyber risk outlining only about 20% of SMEs and 35-70% of larger businesses have standalone cyber insurance.*

In summary

- *Penetration levels for cyber insurance remain relatively modest compared to traditional lines like Property or Liability.*
- *While large corporates typically buy comprehensive cyber coverage, SMEs remain significantly underinsured.*
- *Market penetration is steadily improving due to:*
    - *Regulatory requirements driving awareness.*
    - *Increased media coverage of high-profile incidents.*
    - *Broader broker education initiatives.*

Response from a multinational risk and insurance advisory firm

What do you see as the key challenges in selling cyber insurance or customers buying it? What factors contribute to these challenges

In terms of penetration rates, we can say the SME segment is hovering around 20%, whereas in the ASX200 / large corporate space is approx. 90-95%.

1. Limited Product Awareness & Understanding

- *Particularly SMEs, remain either unaware of cyber insurance or unclear about what it covers, the affiliated services and how it could benefit them. Unlike large corporates, which usually have dedicated risk and security functions and greater exposure to the insurance market, SMEs often lack adequate resources and expertise to fully understand the role of cyber insurance. This limited product awareness contributes to lower uptake among smaller organisations despite their high exposure to cyber threats. We approximate the cyber insurance penetration rate amongst Australian SMEs to be 20%.*
- *Whilst most businesses would acknowledge the need the pre-incident and post-incident services in the event of a cyber-attack, many are not aware that the majority of these critical services are built into the core insurance policy response. Detecting, preventing, and mitigating cyber-attacks before they happen is integrated into the proactive solutions provided by cyber insurers.*
- *Amongst large corporate companies, the product awareness and penetration is much greater, however understanding is often limited on how cyber insurance would practically respond in the event of a real cyber-attack. There is a lack of testing and planning on how an attack would manifest in a business, how insurance plays a critical role in that response, and how stakeholders are engaged as part of the crisis management response.*

2. Previous Pricing Volatility

- *Over the past four years, sharp fluctuations in premiums and capacity have discouraged businesses from taking out cover. The surge in ransomware incidents drove steep market corrections, with significant premium increases and reduced availability of cover. In 2025, the cyber insurance market has now reached a point of equilibrium and stabilisation compared to prior years, rates have remained relatively stable for the past 18 months and we forecast continued stability amongst ample capacity and a competitive market environment.*
- *In particular for SMEs, cyber insurance is often an unexpectedly cost-effective solution for managing cyber risk and having access to a suite of pre & post-incident services.*

3. Security Requirements and Underwriting Friction

- *The hard market years of 2021–2023 were particularly challenging for businesses, as many could not meet insurers' baseline security requirements, and the underwriting process was seen as lengthy and burdensome. The minimum requirements from insurers were in line with recommended best practices as published by the ASD, ASIC and OAIC. Directly as a result of these requirements imposed by insurers, many businesses chose to uplift and invest further in cyber security controls.*
- *Since the market has stabilised, underwriting has become significantly easier, both because of clients improving their security and insurers streamlining their approach, with shorter questionnaires and more focused assessments. Despite this progress, businesses can still be hesitant to engage in the underwriting process.*

4. Trust and Misperceptions

- *A perception problem has developed within the market, with many businesses questioning whether cyber insurance provides value for money or whether claims will be paid. Misleading high-profile media coverage of disputes and exclusions has undermined confidence. The disputes of coverage*

Response from a multinational risk and insurance advisory firm

are often in regards to claims made for cyber incidents under non-cyber policies (e.g. Property, Crime). This is compounded by a mismatch between customer expectations and actual coverage—for example, exclusions for systemic events or state-sponsored attacks—which can lead to the belief that insurance is unreliable or insufficient compared to investing directly in cyber controls.

What would you like to see from Government in terms of recognising its benefits and supporting broader adoption?

1. Cyber Insurance Awareness & Risk Education

- *National awareness campaign to position cyber insurance alongside baseline security controls as part of good risk management.*
- *Promote greater awareness of cyber insurance as a sound risk management tool through collaboration with industry bodies and professional associations. Noting most Australian cyber security standards & guidelines remain technical & based around mitigation.*
- *SME-specific guidance and case studies that highlight the role of insurance in recovery, response, and resilience.*

2. Strengthening Market Confidence

- *Formally acknowledge cyber insurance in national cyber strategies and resilience frameworks as a complement to—not substitute for—security controls.*
- *Support the industry in demonstrating its relevance to the wider economy and society, underlining how faster recovery limits disruption to supply chains, jobs, and services.*
- *Reinforce that the market has matured into a more stable position: S&P Global Ratings recently described the global cyber insurance industry as stable despite increasing competition and incident severity.*

3. Public-Private Partnerships

- *Foster public/private partnerships that allow industry to access de-identified national incident data, improving modelling and long-term pricing stability.*
- *Partner with the insurance industry to target resilience uplift to SMEs/mid-market that cannot adequately protect themselves through cost-effective insurance solutions.*
- *Representation from the insurance industry at relevant government roundtables.*

Strengthen collaboration and consultation between government stakeholders with the private insurance industry to protect Australia's national interest in the event of a widespread incident or crisis, understanding the limitations of the market versus government, including exploration of government-backed systemic risk mechanism. The last couple of years the industry has focused heavily on ensuring that the insurance cover is sufficient and is offered on a sustainable basis.

Response from a global insurance broking and risk advisory firm

One of the key challenges in selling and increasing customer adoption of cyber insurance is the widespread misinformation surrounding coverage, with many companies incorrectly believing that most cyber insurance claims will be denied by insurers.

Response from a global insurance broking and risk advisory firm

Cost remains a significant barrier, particularly for small to medium enterprise, as cyber insurance is often viewed as an optional line of coverage especially when compared to more established policies like public liability or property insurance.

Additionally, the complex and evolving nature of cyber risk leads to varying approaches in discussing and understanding these risks, further fuelling confusion and a lack of understanding of the value cyber insurance can provide.

Key stakeholders in the cyber insurance sector, including brokers and insurers, possess a wealth of cyber risk loss data, and government should encourage increased public-private partnerships to facilitate the sharing of this information. Such collaboration would help improve the overall cyber risk resilience of Australian businesses and highlight the vital role that the insurance industry plays in managing this complex risk.

To address these challenges, government involvement could also help demystify cyber insurance as a product, potentially through incentives or subsidies aimed at small businesses, thereby encouraging broader adoption of this essential risk transfer mechanism.

Response from an international insurance brokerage and advisory firm

While cyber insurance penetration in Australia has improved, it remains low in the SMB and NFP sectors compared to mid-market and corporate who have higher take-up rates. Studies indicate that only around one in five SMB's hold standalone cyber cover, and uptake among micro-businesses is closer to 5%. (Data statistics from CSO Online and Insurance Council of Australia).

For NFP's, particularly smaller community organisations, awareness and adoption are even lower even though they are more likely to be targeted. The insurance and broking sector have already shown it can act as an effective bridge between government initiatives, regulatory requirements, and the day - to - day realities of SMB organisations.

Cyber Insurance Brokers sit in a position of immense trust, guiding business owners through not only insurer and insurance selection but also provide practical steps that reduce risk and improve insurability of these organisations. For many SMB's and NFP's, their first serious conversation about cyber security comes through their insurance broker, often when arranging a renewal or considering cyber insurance as a new policy purchase. This advisory role is now extending beyond risk transfer to include uplift services such as access to vetted IT providers, simple staff training, and preparedness exercises.

Insurers have also evolved with nearly every cyber insurer now embedding incident response hotlines, forensic support, and legal guidance within policy framework - resources that are of great importance but smaller organisations simply could not otherwise afford. Claims data analysis by insurers provides valuable insights into real world attack trends, which can then be fed back into insurer's own underwriting processes as well as client guidance assisting SMB's with valuable and measurable support framework.

The challenges of affordability, perceived complexity, and lack of standardisation are of great prevalence. Many small organisations hesitate to invest in cover they do not fully understand or view as relevant until they experience an incident firsthand. The non-tangible aspect of cyber has been a barrier despite increase in general cyber risk awareness.

Response from an international insurance brokerage and advisory firm

We believe that the government can add value by amplifying the work already being done by insurers and brokers. Recognition of cyber insurance as a legitimate resilience measure (like fire or flood insurance) will help normalise its adoption. Subsidies, grants, or vouchers tied to uplift outcomes could make cover easily accessible as well as incentivise first-time buyers. A government endorsed baseline policy would reduce confusion and help establish trust. Co-branded campaigns highlighting case studies of SMB's and NFP's who successfully recovered with the support of cyber insurance would provide relatable, practical proof of its value.

Insurers and brokers are already delivering advisory benefits to small organisations but with targeted government support, these efforts could scale quickly, driving broader adoption and subsequent measurable uplift in national resilience

Response from an international insurance brokerage

Key Challenges in Selling Cyber Insurance:

1. *Limited Cybersecurity Knowledge Among SMBs:*
   - *SMB owners often rely on their own limited understanding or third-party Managed Service Providers (MSPs) for cybersecurity.*
   - *Many assume their Microsoft environment or MSP agreements fully protect them, leaving them unaware of critical security controls like Multi-Factor Authentication, Encryption, Backup Procedures, or Incident Response Plans.*
   - *SMBs often believe liability is outsourced to MSPs, not realising they remain accountable for cyber risks. MSPs themselves may underestimate the scale of cyber threats, further complicating the issue.*
   - *SMBs may also overlook contractual limitations in third-party service agreements, leaving them to accept constrained liability conditions imposed upon them. This means the risk sits with them.*

2. *Perception of Cyber Insurance Post-2020:*
   - *The hard market of 2020, with reduced capacity and high premiums, created a perception that Cyber Insurance is expensive, limited in coverage, and unlikely to pay claims.*
   - *While the market has since evolved, with 33+ Australian insurers (and various UK insurers) offering broader coverage, competitive pricing, and streamlined processes, this perception persists.*
   - *Insurance brokers play a critical role in educating SMBs and MSPs about the value and necessity of Cyber Insurance, but this remains a challenge.*

3. *Complexity of Cybersecurity and Regulation:*
   - *The evolving cyber threat landscape and regulatory requirements (e.g., penalties for unreported ransomware payments) are difficult for SMBs to navigate.*
   - *Many SMBs lack awareness of resources like cyber.gov.au or struggle to interpret and implement recommended frameworks like the Government's Essential 8.*

4. *Generalist Insurance Brokers:*
   - *Many brokers lack the specialised knowledge to have in-depth conversations with SMBs about cyber risks and the value of Cyber Insurance.*

Response from an international insurance brokerage

- *Cyber Insurers are providing education and resources to brokers, but SMBs still face challenges in understanding and meeting risk management expectations.*

5. *Media Focus on Large-Scale Attacks:*
   - *Media coverage of cyberattacks often highlights large enterprises, leading SMBs to believe they are too small to be targeted or that their data holds no value.*
   - *This false sense of security discourages SMBs from investing in Cyber Insurance.*

6. *SMBs' Limited Resources and Focus:*
   - *SMBs often lack the time, funds, or expertise to prioritize cybersecurity. Their focus remains on growing their businesses, leaving little capacity to address complex cyber risks.*
   - *Many SMBs feel overwhelmed by the fear, confusion, and accountability associated with cyber threats.*

Our Approach:

- *National Cyber Squad: We have established a dedicated Cyber Squad to train brokers, simplify complex concepts, and increase Cyber Insurance adoption across SMBs, medium, and large enterprises.*
- *Education and Support: Ongoing training, branch-level champions, and client-focused conversations aim to bridge knowledge gaps and build momentum in the market.*
- *Advocacy and Collaboration: We advocate for partnerships between the insurance market, businesses, and government to reduce cyber risks, leverage claims data, and protect the Australian economy.*
- *Empathy for SMBs: Recognizing SMBs' challenges, we emphasise support, education, and practical solutions to help them navigate this complex space without detracting from their core business goals.*

By addressing these challenges, we ais to drive greater awareness, understanding, and adoption of Cyber Insurance, ultimately reducing cyber risks and economic losses across Australia.

ANNEXURE C - ATMOS INTELLIGENCE - HARNESSING INCIDENT RESPONSE INSIGHTS AND INFORMATION SHARING TO LIFT RESILIENCE

Please see **enclosed** our latest 'Atmos Intelligence Insights Series' advisory, which we have delivered to the cyber insurance market in Australia, New Zealand and the UK across August 2025.

To explain the background context of our latest advisory, we collected 100+ datapoints for all incidents that we are engaged to assist with. Our in-house threat intelligence team reviews this data, and after de-identifying it, imports it into our protected dashboard which we use to harness our learnings for presentation back to the industry.

In summary of our findings over the last quarter:

a. **Ransomware and Business Email Compromise events make up the highest proportion of incident types** – with a notable focus on third party breaches and rogue employee / insider attacks.

b. **Micro and Small Businesses (revenues up to $10m) are disproportionately affected by cyber incidents** – accounting for nearly 50% of incidents. These organisations are often unable to weather the costs of cybercrime and cyber incidents (without insurance).

c. **Mid-market, Large and Enterprise businesses (revenues $10-$100m, $100m-$1bn, and $1bn+)** – account for the remaining 50% of incidents, typically experiencing an increased severity compared to smaller organisations.

d. **All industries are targeted, some more so than others** – Financial Services, Professional Services, Retail, Health and Construction are the top 5 impacted industries, with a cross-representation by other industries.

e. **2025 has seen a busier than usual start to the year** – 2025 has remained on par with previous year's activity despite various efforts to slow down the frequency of cyber incidents.

f. **Threat actors continue to multiply** – despite disruption efforts, sanctions, takedowns and other law enforcement efforts, threat actor groups continue to spawn, splinter and spread. It is becoming much more difficult to track this activity and 'understand the adversary' with emerging groups constantly forming.

g. **Notifiable data breaches don't always occur** – not every cyber security incident is a reportable data breach, although where a data breach occurs, concern tends to focus on data which can't be remediated through protective measures. This predominately includes health information.

h. **Funds transfer fraud is a drag on our economy** – despite being the incident type that doesn't grab headlines, business email compromise incidents and associated social engineering fraud / funds misdirection results in millions of dollars being stolen from our economy each year (mostly from small businesses). Average payments this quarter were $26,000 (this is much less than usual) with the largest amount being more than $2m, leading us to observe a trend of 'big game BEC hunting' for larger organisations.

i. **Time to detect is becoming shorter** – the average dwell time (the time between when unauthorised systems access occurs and when it is identified) is approximately 8 days for ransomware events. This is shorter than usual timeframes of 10-24 days, which is a good thing, but still enough time for threat actors to do damage (steal data or encrypt). Notably, the Akira / SonicWall vulnerability has caused a spike in incident activity in the past quarter, as has the efforts of Scattered Spider.

j. **Ransom payment frequency is decreasing** – our statistics show that approximately 15% of organisations pay a ransom demand, which is down from about 30% or organisations that paid one year ago. That said, demands overall are increasing to account for this. Efforts to counteract payment include better response resilience, injunctions, and the ransomware payment reporting framework. Average demands however are about $1.2m with average payments being about $430,000 for the quarter.

While other statistics are available to the market (including the annual ACSC's Annual Cyber Threat Report) this is a good example of where law firms, DFIR firms, and the insurance industry can be leveraged to obtain information to help inform the public policy considerations for further investment.

Atmos Intelligence Insights Series

August 2025

Atmos

Key highlights this quarter

25+

INDUSTRY PRESENTATIONS SHOWCASING CYBER INSURANCE RESPONSE LANDSCAPE

4

MANDATORY RANSOMWARE PAYMENT REPORTING ENGAGEMENTS

3

CHATGPT BREACHES: A RISING CONCERN

$1.5m+

RECOVERED FROM FUNDS MISDIRECTION

67+

TEAM MEMBERS AND GROWING

June

OFFICIALLY LAUNCHED NEW ZEALAND OFFICE

August

HORIZON 2 CYBER SECURITY STRATEGY SUBMISSIONS DUE

2026

CYBER CONFERENCE PLANNING- DETAILS COMING SOON

Global landscape

THREAT LANDSCAPE

Law enforcement

New threat actors

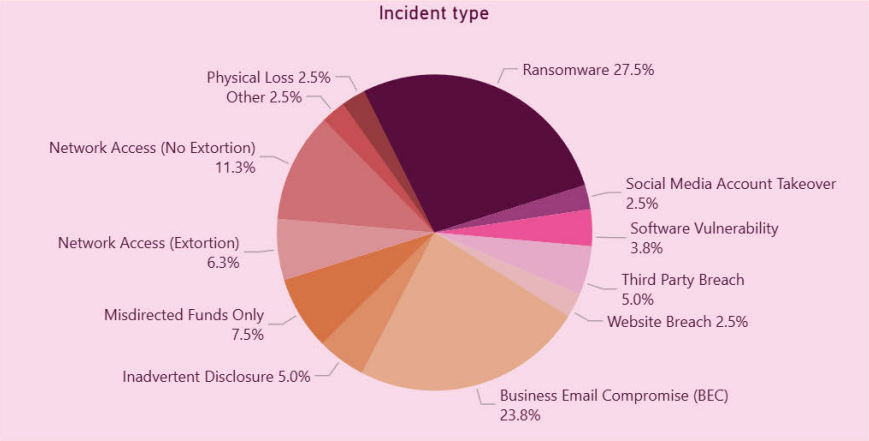
Volatile landscape

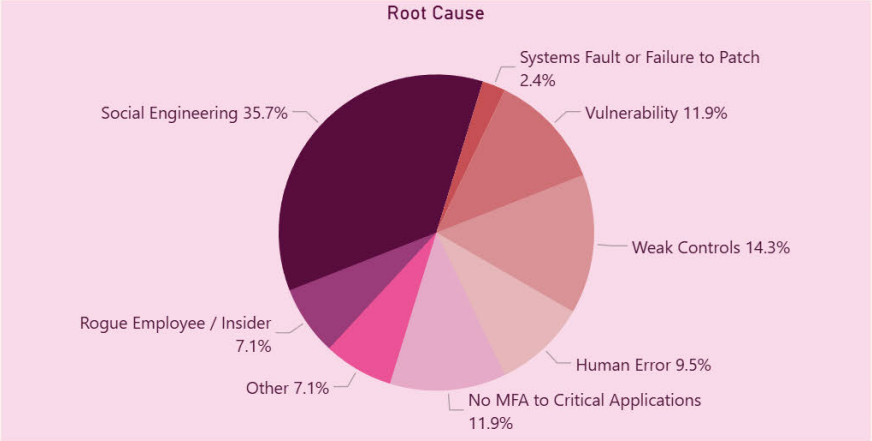
Atmos

Incident overview

INCIDENT TYPES AND ROOT CAUSE

- Ransomware / extortion incidents the highest frequency incident type **(27.5%)**
- Business Email Compromise close second **(23.8%)**
- Social Engineering is the leading root cause **(35.7%) – increasing trend**
- Other causes of loss: weak security controls **(14.3%)**, unpatched vulnerabilities **(11.9%)** and no MFA to critical applications **(11.9%)**
- Increase of rogue employee/insider **(7.1%)** and human error **(9.5%)**

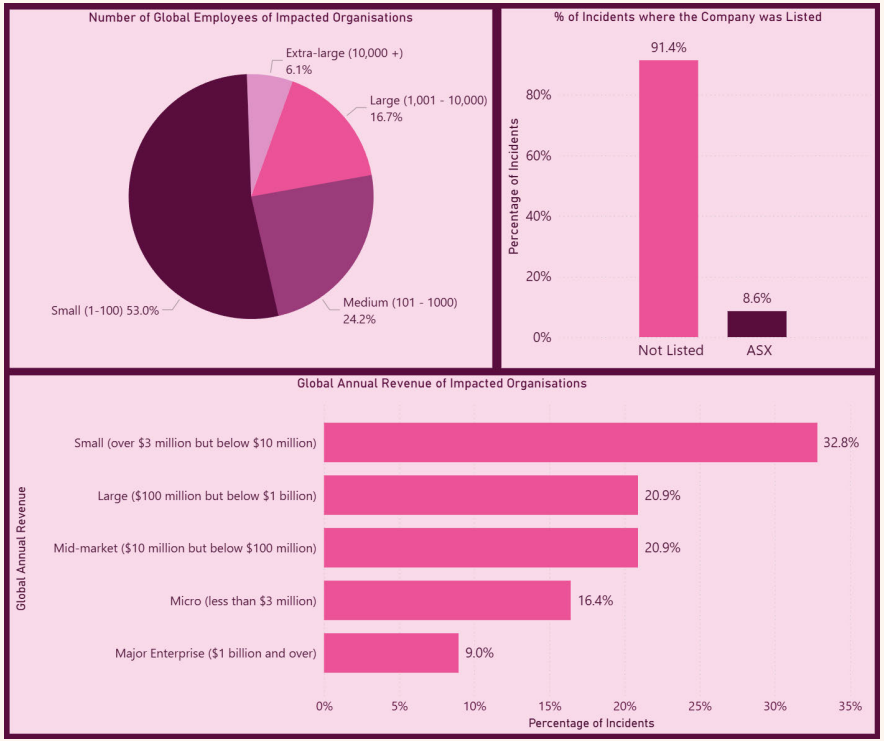




Victim profile

SIZE AND PROFILE OF IMPACTED ORGANISATIONS

- Mixture of government, private and public companies
- Mixture of Australia / New Zealand domiciled and international / APAC entities across all sectors
- Small businesses most commonly impacted:
  - 1 to 100 employees (53%) and 101 to 1001 employees (24%)
  - <$3m (micro) and $3-10m (small) = nearly 50%
- Mid-market, large and enterprise combined = 50%
- Validates concerns that small businesses are targeted most frequently and require additional support
- Mid-market, large and enterprise organisations also experience greater severity exposure, typically with higher impact incidents
- Emerging focus on State Government and contracted service providers (QLD, NSW, WA) with privacy law reform washing through
- Continued focus on SAAS / MSPs and B2B aggregators

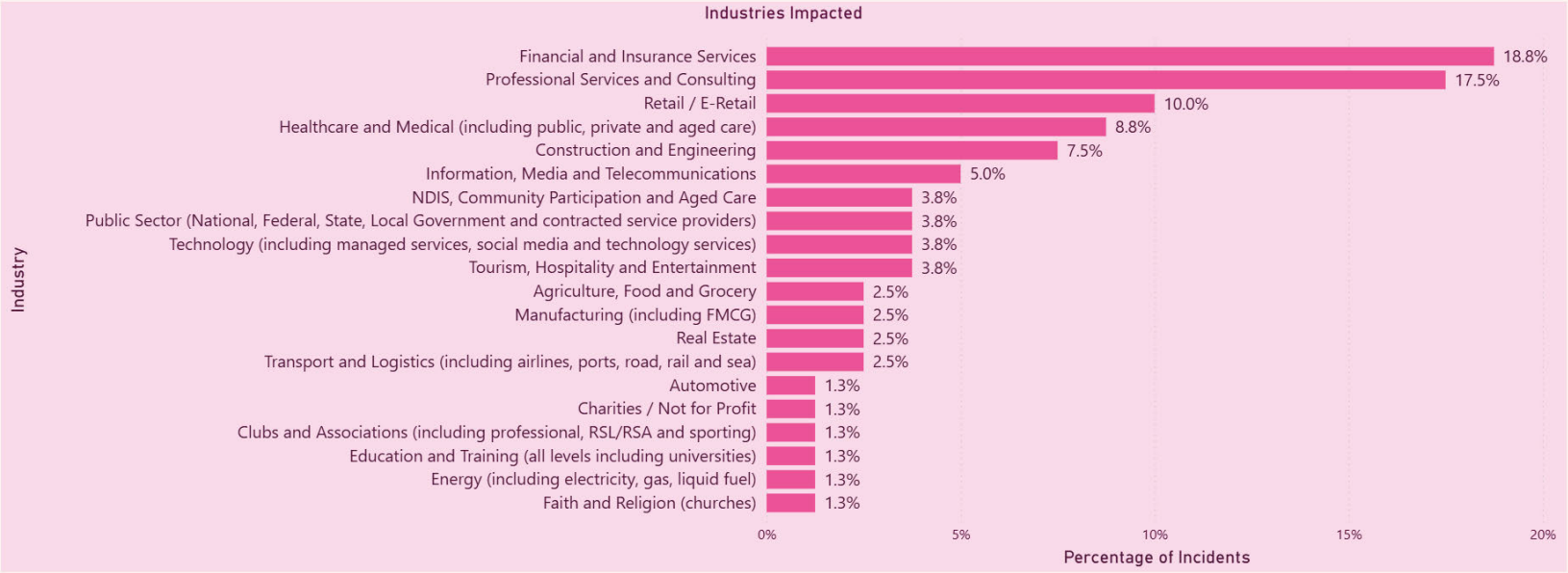


Atmos

Industries targeted

BREAKDOWN OF INDUSTRIES IMPACTED

- Financial and Insurance Services **(18.8%)**, Professional Services and Consulting **(17.5%)**, and Retail **(10%)** were the top industries impacted
- Broadly speaking – mixture of industries with a focus on real world impact ('all hazards approach' to cyber, privacy and digital risk) including operational resilience

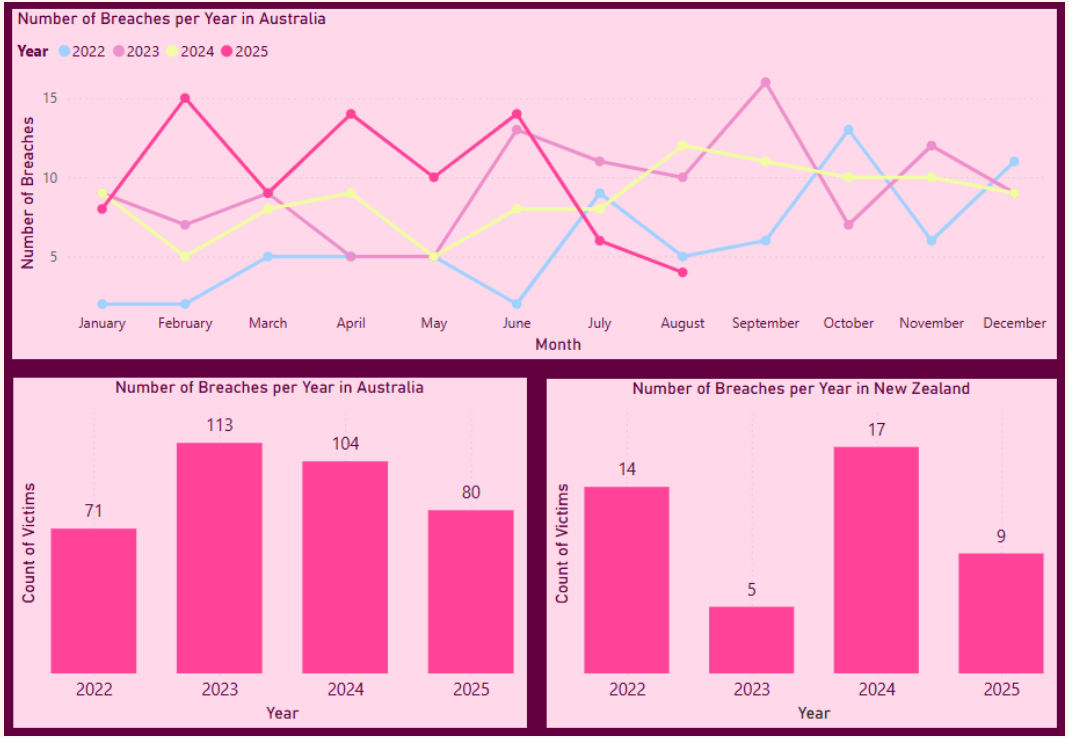


Dark web activity

VOLUME OF ACTIVITY

- Indication of cyber incident volume
- Year on year analysis of dark web ‘breaches’ for Australia and New Zealand organisations
- Includes access broking or data being leaked/offered for sale, and dark web leak site mentions/posts
- While this won’t reflect the true volume of overall incidents, this does give an indication of activity frequency which continues to remain on par with recent years
- Overall observation: busier than usual start to 2025 in Australia – geopolitics at play?
- Typically now is the ‘busy season’ between September to November based on previous experience with December to February being quieter

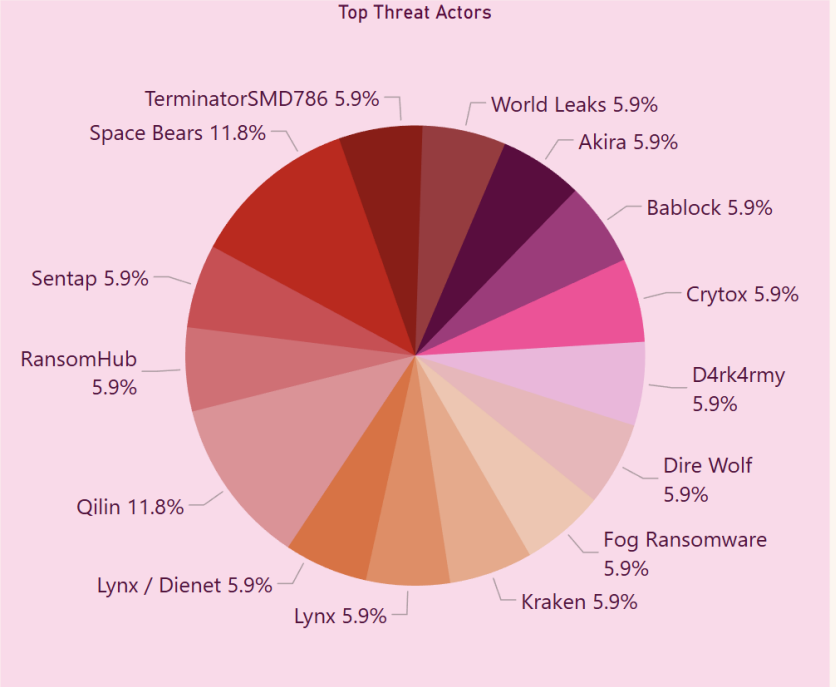
Source (Intel 471)



Threat actor profile

THREAT ACTOR TRENDS

- The threat actor landscape remained highly diverse with a broad distribution of attack sources rather than domination by a single threat actor group (note: See Coveware where Akira, Qilin, Lone Wolf dominates)
- From January 2025 to July 2025, **41** new ransomware groups were observed to be running data leak sites, a **41%** increase from the same time last year when **29** new ransomware groups were detected
- Qilin **(11.8%),** Space Bears **(11.8%),** and Akira **(5.9%)** ransomware groups were the most active threat actor groups. Akira is particularly active now, exploiting the SonicWall vulnerability
- Evolving extortion tactics including
  - More frequent threats to engage prominent media outlets to discuss the incident
  - Operating call centers in multiple languages to target victim organisations and their customers, and leave harassing voicemails
  - Reviewing stolen data for incriminating evidence and subsequently threatening to send to law enforcement, tax authorities and industry regulators, making negotiations difficult

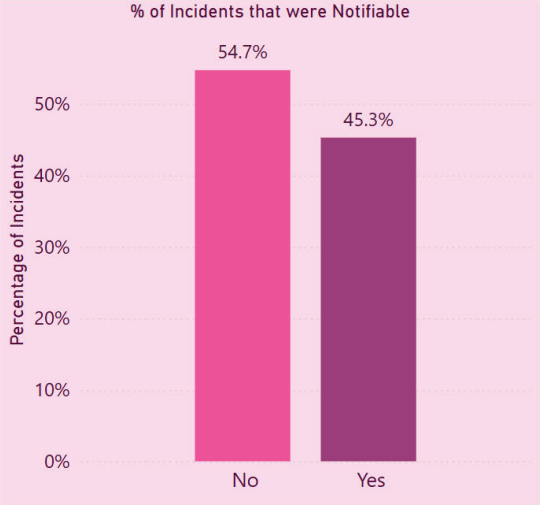


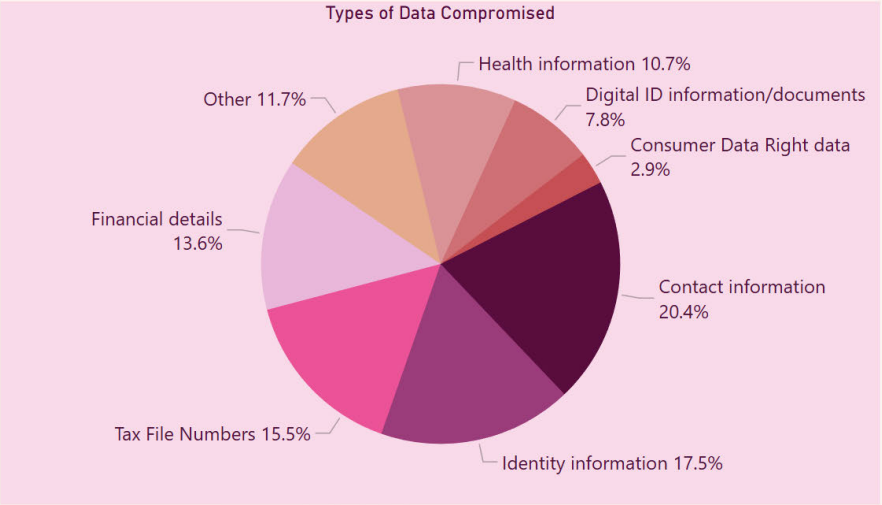
Atmos

Data impact trends

NOTIFICATION TRENDS

- Nearly half **(45.3%)** of incidents were notifiable data breaches – mosaic effect in people's minds with Digital ID changes likely to reduce harm
- Contact information **(20.4%)**, identity information **(17.5%)**, and Tax File Numbers **(15.5%)** remained the most frequently compromised data types
- Health information **(10.7%)** was lower in proportion this quarter although often causes the most concern and claims risk (see IVF class action)



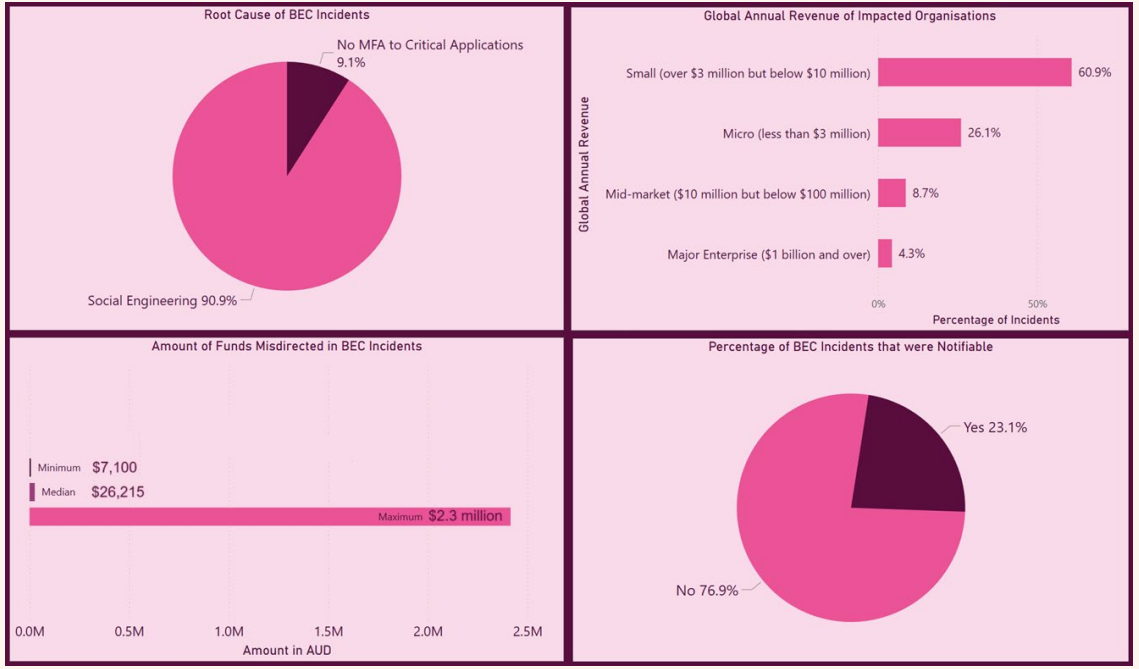


Atmos

Business Email Compromise in focus

KEY HIGHLIGHTS

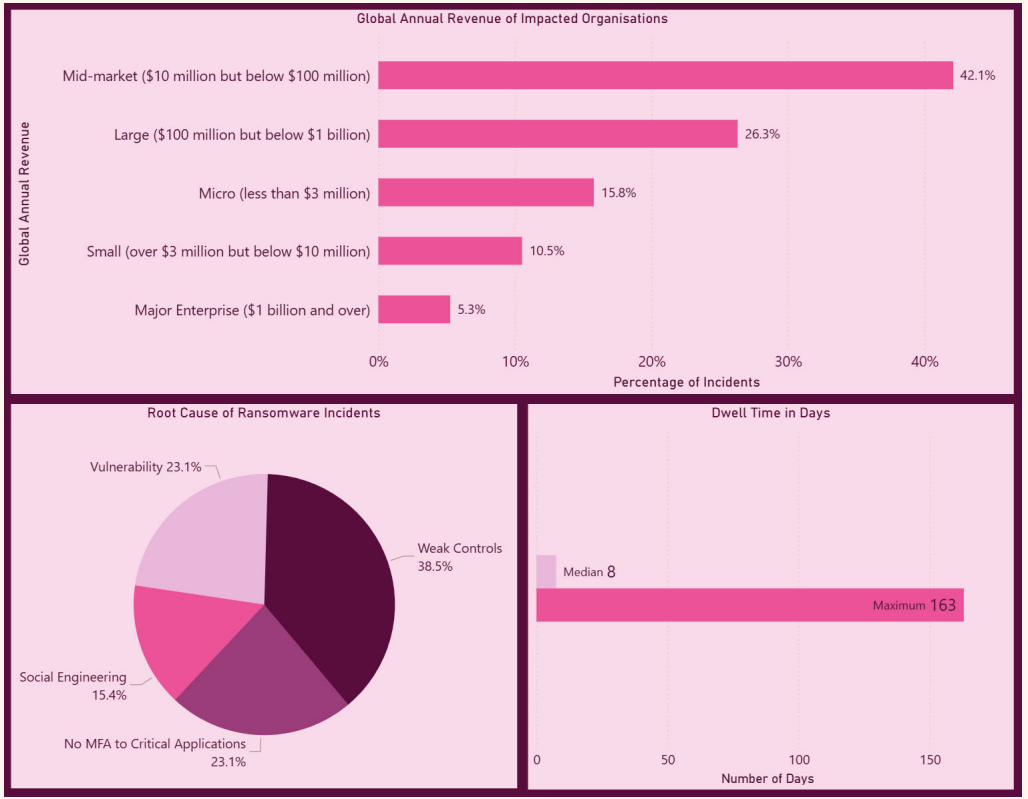
- Micro and Small Businesses are over-represented by Business Email Compromise and Funds Transfer Fraud incidents
- While this isn't new trend, it is a focus area for the Atmos Resolve team which is committed to supporting the small business sector with this drag, and funds recovery efforts
- We have assisted multiple Enterprise clients – with attempted large loss funds transfer fraud events (>$10m) indicating a growing trend towards 'big game BEC hunting'
- The median amount of funds misdirected was **$26,215**, while the largest amount of successful funds misdirected was **$2.3 million**
- **$1.5m** successfully recovered through our Atmos Trace Now team – super stoked



Ransomware in focus

ROOT CAUSE AND SIZE OF ORGANISATIONS IMPACTED

- Organisations of all sizes were impacted; indicating that attacks are largely opportunistic in nature
- Threat Actor 'dwell time' aka 'time to detect' (which refers to the period between when a threat actor first gains unauthorised access to a system and when they were detected) has **significantly reduced**
- The minimum 'dwell time' was **0 days**, while the median dwell time observed was **8 days**, and the maximum dwell time that was observed was **163 days – this is typically ~10-24 days**
- This is actually a good thing – it shows that organisations have increased detection capabilities
- As a result – threat actors are getting much quicker at getting in and stealing data before they leave, often without encrypting networks (extortion only attacks)
- Coveware has noticed an uptick of this 'data theft only' attacks and lone wolf attacks

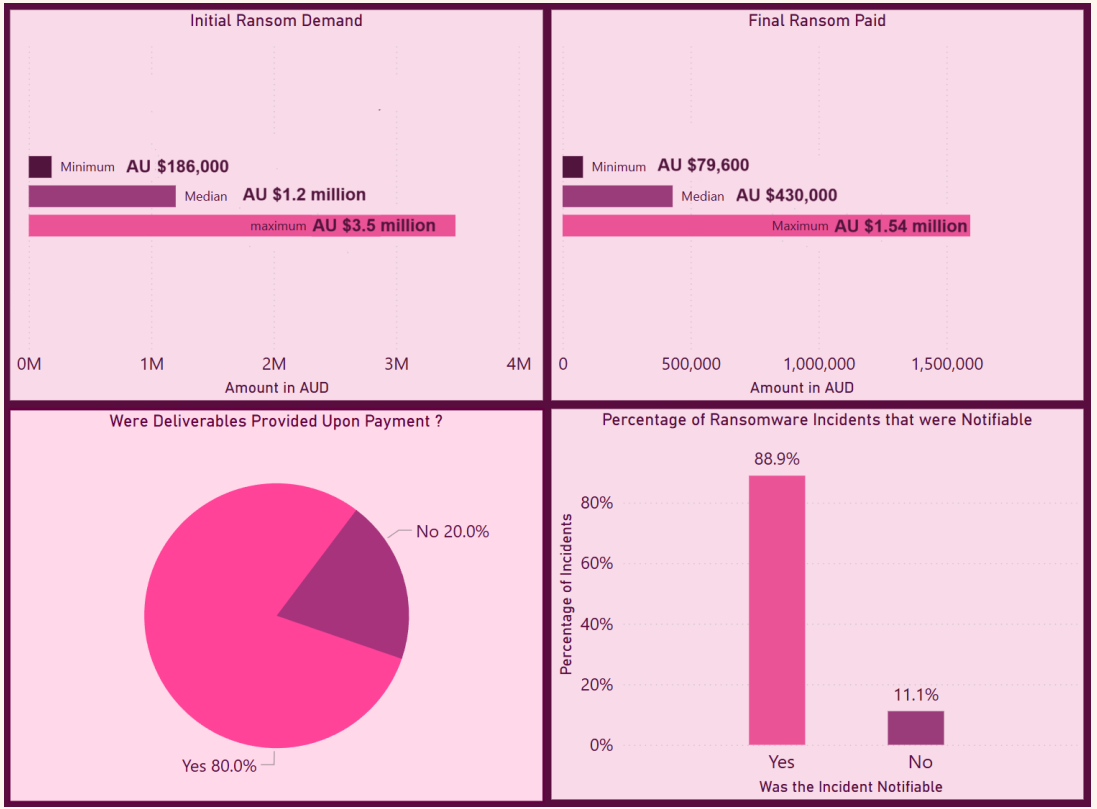


Atmos

Ransomware in focus

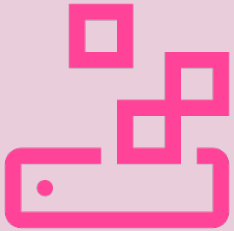
NOTIFICATIONS AND RANSOM DEMANDS

- The median initial ransom demand that was observed was **AUD $1.2 million**, while the median ransom payment was **AUD$430,000**
- The maximum initial ransom demand observed was **AUD$3.5 million**, while the largest ransom payment was **AUD$1.54 million**
- This aligns with higher frequency, lower demands overall compared to previous years but see Coveware: increased spike in demands + payment amount
- In ransomware incidents where a ransom payment was made, deliverables were provided in **80%** of cases, while no deliverables were provided in **20%** of the cases (SpaceBears) where re-extortion occurred
- This is an anomaly to usual behaviour – but reflects the growing nature of 'new groups' which are less organised, and less trustworthy



Things to look out for

Limit adequacy,
BI, claims



SonicWall + Akira

Emerging Tech

Where to from here

- ONBOARDINGS - [redacted]!
- COLLATERAL UPDATE - Chat to [redacted]!
- FOLLOW US ON LINKEDIN for more

First Response

Atmos

65+

Team members to support you

2,500+

Incidents handled

5

Offices across Australia and New Zealand

100+

Specialist partners to help you in your journey