Submission – Lockton Australia Cyber Practice Leader

For: Department of Home Affairs – Developing Horizon 2 (2026 - 28)

Executive Summary

Lockton Australia welcomes the opportunity to contribute to the co-design of Horizon 2 of the 2023 - 2030 Australian Cyber Security Strategy.

As the largest privately held global insurance broker and one of Australia's leading cyber, data and technology sector insurance advisory practices, we are uniquely positioned at the intersection of risk transfer (insurance), advisory, and operational resilience.

Cyber insurance is not simply a post-loss financial product - it is a business enabler that can drive measurable improvements in cyber maturity, resilience, and economic competitiveness when strategically integrated with national policy.

Our Inform – Improve – Insure framework (elaborated throughout) demonstrates how cyber insurance, drives posture uplift and resilience for both entities (SME to large Corporate, across all sectors) and the broader economy.

There is an opportunity with Horizon 2 to embed insurance mechanisms into the six shields, creating economic resilience, stronger governance, and digital trust. Tangibly this requires:

a. Government to actively recognise and advocate for the role of cyber insurance as a core pillar of national cyber resilience.

b. Mandate structured, reciprocal data sharing and joint working groups between govt. and the insurance sector leveraging claims insights/threat intelligence.

c. Introduce compulsory cyber insurance for SMEs in high-risk or priority sectors where incidents have the greatest economic and community impact.

d. Progressively mandate cyber insurance for all Australian organisations, modelled on compulsory Workers Compensation, ensuring universal baseline protection.

All recommendations are designed to preserve fair competition, avoid moral hazard, and complement—not replace—existing ACSC standards

In aligning with the key pillars, our submission advocates for:

a. Embedding insurance enablement into Horizon 2 delivery – using insurance market levers to incentivise and accelerate maturity uplift across all sectors, especially SMEs.

b. Building an integrated workforce and advisory ecosystem – bridging technical expertise, policy knowledge, and commercial risk advisory capability.

c. Leveraging insurer–broker–client-breach coach-threat intelligence loops – ensuring data from catastrophic claims, small claims and near-misses feeds directly into prevention and resilience measures.

We propose specific suggestions including pilot schemes, quantitative maturity frameworks, shared risk pools, and insurance industry participation in threat sharing frameworks.

We look forward to working with the Department of Home Affairs, ACSC, ASD and other stakeholders to deliver scalable, market-aligned, and sustainable outcomes consistent with Australia's ambition to be a world-leader in cyber security by 2030.

[redacted]

[redacted] | global.lockton.com

MEMBER OF THE Tech Council Partners Forum

CORPORATE AISA PARTNER

Key recommendations

Specific Questions addressed and Lockton response

Consultation Question	Lockton Recommendations/Proposal
2. Developing our vision for Horizon 2 - 2.1 Outlook for Horizon 2	
1. What trends or technology developments will shape the outlook over the next few years and what other strategic factors should Government be exploring for cyber security under Horizon 2?	Recognise the value and contribution the insurance industry can make to meeting Australia's Cybersecurity strategy, more actively engage and involve the sector. Recognise insurers as "proxy regulators" raising baseline controls (MFA, EDR, patching, IR testing). Acknowledge and support innovation in "Active Insurance" (continuous monitoring, vulnerability alerts, fraud recovery). Leverage insurance claims data to inform national resilience planning.
3. Shield-level focus for Horizon 2 - 3.1 Shield 1: Strong businesses and citizens	
3.1 Shield 1: Consolidate our cyber awareness messages across the economy?	Government to explicitly recognise and advocate for cyber insurance as a resilience enabler. Embed myth-busting in awareness campaigns (e.g., insurers pay claims with accompanying data). Produce plain-English materials explaining how cyber insurance responds (first-party, third-party, incident response). Add an "Insurance & Resilience" insert to ACSC awareness materials.
3.1 Shield 1: Increase cyber literacy in our schools and early learning programs?	Develop a simple "risk & resilience" module in the Year 9–10 curriculum (covering cyber hygiene and insurance as a risk-pooling tool). Commission ACARA to deliver a micro-unit linking digital safety with recovery and resilience.
3.1 Shield 1: Target resilience uplift to SMEs and NFPs that cannot adequately protect themselves, including through tailored cyber security standards that are cheap to apply?	Introduce Cyber Uplift Voucher pilots (co-funded maturity assessments + insurance readiness). Publish an insurer-aligned SME/NFP baseline (8–10 core controls mapped to Essential Eight/SMB1001). Provide tiered, insurance-linked incentives for incremental posture improvements. Expand access to insurer/broker incident response panels so SMEs/NFPs can access expert services at scale
3.1 Shield 1: Enhance support for citizens and victims of cybercrime to help them bounce back quicker?	Leverage insurers' 24/7 incident response panels (forensics, legal, PR) that often engage below deductibles. Establish an Identity Restoration Pathway using insurer panel providers (credit monitoring, document replacement support) for citizens impacted by insured SME/NFP breaches.
3.1 Shield 1: Harmonise and simplify cyber regulation to promote best practice and efficiency?	Align SOCI, Privacy Act and ransomware reporting thresholds/timelines with common insurance notification norms. Introduce safe-harbour provisions for entities meeting insurer-recognised maturity baselines (reduced penalties, streamlined reporting).

Documents referenced include Page 6 of Charting New Horizons Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy and questions 5 – 6 under 3.1 Shield 1: Strong businesses and citizens of Appendix A: List of questions to consider when making a submission

Cyber Insurance – Context and position as an enabler

Summary

Strategic Context

Why Insurance Matters

- **Individual organisation perspective**
  Cyber Insurance uplifts awareness, enables strategic initiatives (M&A, new products), and provides fiscal safety nets.
- **Broader economic perspective**
  Cyber Insurance reduces systemic distress, preserves jobs, and underpins investment.
- **Governance perspective/role as proxy regulator**
  Cyber Insurance demonstrates prudent risk transfer. Market sets baseline standards using claims data, driving posture uplift.
- **Data**
  Cyber Insurance claims data and intelligence assists to identify posture gaps, leading to direct investment into the most value-adding controls. In turn this strengthens governance, resilience, and digital trust.
- **Incident Response**
  Cyber Insurance facilitates access to leading incident response capabilities from a legal, technical and other standpoint, significantly reducing the impact of cyber events on individual organisation's and the economy more broadly.

The transfer of risk, from Australian's organisation's balance sheet to insurers not only plays a key role as part of these organisation's broader risk management programs (safeguarding from catastrophic financial, operational, and reputational risks), but can, and should also act as a broader business enabler, for those entities, and the broader Australian economy.

Cyber Insurance

Overview

Cyber insurance is the primary way organisations can transfer the financial, operational, and liability risks of a cyber incident off their balance sheet. It operates across three key areas of protection:

First-Party Protection

Covers the organisation's own direct costs when an incident occurs. This includes incident response and recovery expenses, data and system restoration, forensic costs, and business interruption losses. It ensures the organisation has both the capital and specialist support to recover quickly.

Third-Party Liability Protection

Responds to claims made against the organisation by others, including regulatory investigations and fines, customer or partner liability, media and IP disputes, and other legal or contractual exposures. This protects both the entity's financial position and the personal liability of directors and officers.

Incident Response Enablement

Provides immediate access to 24/7 expert support panels, including forensic investigators, legal advisors, crisis PR firms, and breach coaches, at insurer-negotiated rates. This is often one of the most valuable aspects of cover, as it gives organisations access to resources and expertise they could not easily afford or mobilise on their own.

Background of the Australian Cyber Insurance Market

Gross Written Premium (GWP) - Size

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.

Cyber risk - Insurance Council of Australia

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.

Insurance misconceptions

Elaborated page 16, the idea that "cyber insurance doesn't pay" is a misconception driven largely by misunderstandings and isolated disputes under traditional insurance policies never designed to cover cyber losses.

In reality, standalone cyber policies are highly responsive when aligned to an organisation's risk profile:

- In 2024 Australian insurers paid around AUD $247 million in cyber claims, and
- Global leader CFC confirmed it paid 99.1% of claims submitted.

Peer-reviewed research supports this, showing that only 5% of reported disputes relate to standalone cyber policies, with most linked to general liability or property policies, and that media coverage has skewed perception by focusing disproportionately on rare "war clause" cases.

The evidence clearly demonstrates that cyber insurance does pay and is a reliable tool for transferring cyber risk and enabling resilience.

Cybersecurity investment vs Cyber Insurance

Elaborated page 17, cyber security investment and cyber insurance are two sides of the same coin. Strong governance, technical defences, and awareness programs reduce the likelihood of incidents, but no organisation can fully eliminate risks such as zero-day vulnerabilities, supply chain compromises, insider threats, or state-sponsored activity.

Cyber insurance complements these efforts by transferring the unpredictable and catastrophic exposures that remain, ensuring access to capital, continuity, and expert response. Rather than competing, security controls and insurance create a whole-of-event safety net - prevention at the front end, and protection and recovery at the back end. In practice, organisations benefit twice: from reduced frequency of incidents through effective controls, and from the financial protection, incident response, and coverage advantages that insurers provide when those controls are in place.

Together, investment and insurance create a virtuous cycle that strengthens resilience for organisations, individuals, and the broader economy.

Why Insurance Matters

Individual organisation perspective

For individual organisations, effective risk transfer can

a. Uplift cyber awareness and maturity
b. Facilitate opportunity, i.e.,
    a. Strategic initiatives (such as acquisitions), or
    b. Product or service expansions

by the very nature of it acting as a fiscal safety net.

Broader economic perspective

For the broader economy Cyber insurance can play an integral, foundational role for economic resilience. By protecting balance sheets and preserving access to capital, insurance

a. Reduces the broader economic risk of corporate distress,
b. Safeguards jobs, and
c. Supports continued investment and innovation.

Enabling the scaling of the broader cyber ecosystem.

For trade and investment, cyber insurance underpins M&A, financing, and contractual certainty, making organisations more competitive globally. Importantly, the cyber insurance market acts as a proxy regulator, using claims data to define minimum standards and guide uplift in posture across the economy. This not only accelerates national cyber maturity but also fosters digital trust - a proven driver of customer confidence and revenue growth.

Governance perspective/role as proxy regulator

Cyber insurers can positively influence cybersecurity measures at companies, acting as proxy regulators by requiring certain minimum levels of security from companies for the insurance cover they provide (MacColl et al.,). Cyber insurance requires minimum security controls of organisations, or for them to address "issues" addressed before a policy is active (or within a timeframe), continuously – by example - giving extra incentives for organisations to keep updating, patching, and to practice defense-in-depth.

Data

Providing a fiscal safety net, accompanied with access to a 24/7, 365 panel of leading cyber response experts on personal retainer for an organisation are now well-known benefits for implementing a cyber insurance policy.

Less well known, but now more pertinent than ever, is that the implementation of a policy, and the work involved in ensuring an organisation has a cybersecurity posture that meets minimum standards can, and does offer clear guidance and direction as to broader best cyber security practice standards.

The global cyber insurance market is using the data it holds from the diverse and arguably incomparable pool of claims, losses, and associated causes to offer insight into what best cybersecurity practice looks like. This translates to guidance and incentives to business – in the form of eligibility, pricing, and sharing of insights – on best cyber security practice standards.

When organisations face the question of where to begin with cyber security investment, leveraging insights from the cyber insurance market provides a powerful, evidence-based starting point. Insurers and underwriters bring a unique perspective, informed by real-world claims data and loss experience, that extends well beyond technical costs alone. Their analysis captures the whole-of-event exposure - immediate technical response, first-party financial loss, and third-party liability - highlighting the true scale of cyber incidents on businesses and communities.

Incorporating these insights ensures that cyber security strategies and capital allocation are directed to the controls, practices, and procedures most effective in reducing both the likelihood and impact of catastrophic events.

Incident Response

For SMEs/NFPs, insurer panels provide immediate access to forensic, legal and crisis communications expertise at negotiated rates, often engaging below deductibles. This materially shortens time-to-containment and reduces both direct and indirect costs (downtime, reputational harm), and is frequently the most valuable aspect of the policy for smaller organisations with limited in-house capability. Government recognition of insurer panel access and routing victims to these services quickly is a public-interest resilience asset.

Examples where insurance provides quantifiable insights

Example #1

A study by an internationally leading insurance market combined two datasets:

- Cybersecurity posture questionnaires (Proposal Forms) for individual organisations
- Historical claims data from November 2020 to November 2021, consisting of
    - Claims events that resulted in a cyber claim being paid, and
    - Notices of circumstances that didn't cause an insured loss.

The insurer used the two datasets to look at which cybersecurity controls have the greatest effect on decreasing the likelihood of an organisation experiencing a cyber event.

The result was discovery of consistent controls, practices and procedures, that were consistently correlated with a reduction in or no loss incurred by an insured.

Example #2

The second study focused on the cyber controls implemented by small and medium-sized enterprises (SMEs). The insurer cross-checked and validated the controls identified in the study against information gathered from its SME customers proposal forms, as well as benchmarking data from global customer assessments and claims.

The insurer found a direct correlation between 10 controls that mitigated 70% of the most common SME cyber risks.

Example #3

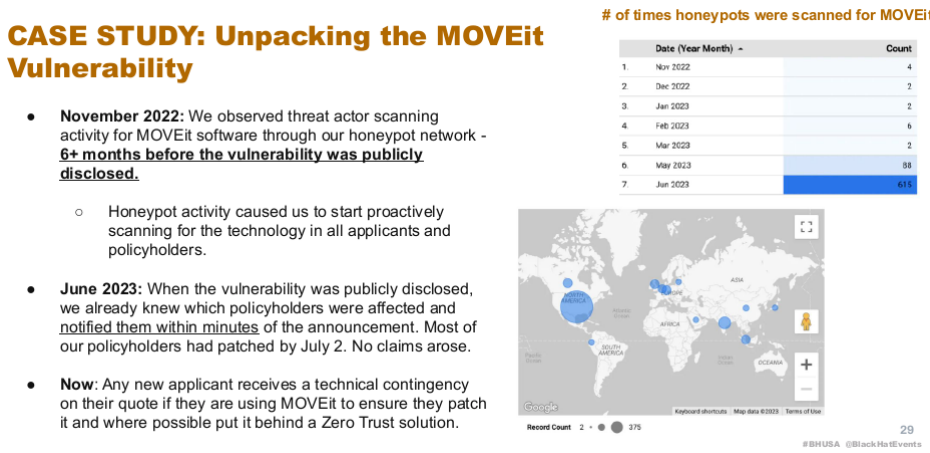
Coalition (a globally respected, leading Cyber Insurer) implement an Active Insurance approach that incorporates continuous Risk Assessments, Active Protection, and Active Response, providing policyholders with holistic benefits in protecting their organisations against dynamic risks.

Active Insurance is coverage designed to prevent digital risk before it strikes. Unlike traditional insurance, designed only to cover and transfer risk when the worst happens. Active Insurance provides continual risk assessment, monitoring and response to address risks that move at digital speed.

Daniel Woods, a key Coalition figure head, recently provided a key case study "How Cyber Insurers Incentivize Security: Past, Present and Future" which outlines how Coalition shapes cybersecurity for organisations via:

- Coverage innovations like vanishing retention
- Clawing back over $100m of fraudulent funds stolen by criminals
- Sending zero day alerts about vulnerabilities under active exploitation
- Studying claims to identify common ransomware attack vectors and helping firms fix these

A further example of the value their Active Insurance stance provides, is outlined below.



Example #4

"Policyholders Have Better Security Outcomes" - Forrester

Forrester found that the tighter standards set to qualify for cybersecurity insurance have better data breach response times.

According to Forrester's findings, there's a recurring pattern of improved detection and response for organizations with standalone cybersecurity insurance policies. Regarding the mean time to detect a breach (a common metric), 25% of global enterprise respondents with standalone cyber insurance policies reported that they could do so in seven days or fewer, compared to 19% of those without cyber insurance.

Similarly, 29% of those with a standalone cybersecurity insurance policy can respond to breaches within seven days. compared to only 19% without cybersecurity insurance.

Other areas of improvement include breach or malware eradication times and overall recovery from incidents. Finally, those with cybersecurity insurance are more likely to be further underway in building zero-trust architectures than those without insurance.

Cybersecurity Insurance: Signals Maturity to Partners, Improved Security Response - Security Boulevard

Example #5

"Insurers have 'a check' role in fight against cyberwashing"

A growing concern is the rise of "cyberwashing" - where organisations overstate or misrepresent their cyber security credentials to regulators, stakeholders, or customers, creating a false sense of protection.

This practice undermines trust and increases systemic risk.

Cyber insurance can serve as a practical safeguard against cyberwashing, as insurers require accurate disclosure of controls during underwriting and may deny or void cover if misrepresentations are discovered.

In this way, the insurance market operates as a market-based accountability mechanism, complementing regulatory enforcement by ASIC and the Notifiable Data Breach scheme. Recognising and embedding this role of insurance within Horizon 2 would strengthen the integrity of cyber security disclosures, reduce information asymmetry, and foster greater digital trust across the economy.

Insurers have 'check' role in fight against cyberwashing - Insurance News - insuranceNEWS.com.au

Value translated

Translated, Lockton's Inform – Improve – Insure framework helps demonstrate the operationalisation of the value of cyber insurance, for both organisations and the individuals who govern them.

Inform	Improve	Insure
Translate cyber risk into business language for boards and executives. Helps entities prioritise finite resources.	Uses insurer claims data and intelligence to identify posture gaps. Direct investment into the most value-adding controls. Strengthen governance, resilience, & digital trust.	Protects balance sheets. Preserves access to capital and safeguard operations, reputation, and competitiveness. Provides access to world-class incident response and recovery services.

Horizon 2 Alignment

By pooling and redistributing systemic risks, cyber insurance strengthens national resilience, ensuring that cyber shocks do not derail prosperity. Insurance - like cyber, data, and technology risk – is not static, but a strategic enabler of resilience, growth, and economic strength. In this way, insurance directly supports Horizon 2's objectives in scaling national cyber maturity, empowering SMEs and NFPs to make cost-effective, prioritised, informed decisions informed and embedding resilience across society.

Through this lens, cyber insurance is not merely a mechanism for risk transfer - it is a strategic enabler of Horizon 2's mission to expand reach, uplift capability, and strengthen economic resilience. It achieves this by creating the financial and operational certainty that allows organisations to invest, innovate, and recover with confidence. Importantly, however, cyber insurance can only fulfil this dual role - as both a protective buffer and a driver of national uplift - if it is:

- Structured and implemented cost-effectively – Policies must remain accessible, particularly for SMEs and NFPs, to avoid perceptions of exclusivity and to ensure broad-based adoption across the economy.
- Aligned with organisational risk appetite – Coverage should reflect the unique risk profile and tolerance of each organisation, ensuring that risk transfer complements, rather than distorts, business decision-making.
- Understood in its operation and response – Organisations must be clear on how cyber insurance responds, the scope of cover, and the critical role of incident response services, so that it is seen as a reliable enabler rather than a misunderstood expense.
- Supported and facilitated by government while preserving the free market – Government has a role to play in recognising cyber insurance as a pillar of national resilience, creating incentives for adoption, aligning regulation with market practice, and embedding insurers in threat-sharing and policy design, all while maintaining a competitive marketplace.

In this way, cyber insurance can move beyond being perceived as a back-end financial product and instead be recognised as a whole-of-economy resilience mechanism, central to the delivery of Horizon 2's objectives.

Lockton Recommendations

Horizon 2 Vision and Outlook Recommendations/Levers

2. Developing our vision for Horizon 2 - 2.1 Outlook for Horizon 2

What trends or technology developments will shape the outlook over the next few years and what other strategic factors should Government be exploring for cyber security under Horizon 2?

Governance & Co-design Integration

Establish a Cyber Insurance Advisory Panel within the Executive Cyber Council, ensuring the insurance market is a standing contributor to Horizon 2 program reviews.

Mandate annual joint reporting from government and the insurance sector on maturity progress, claims trends, and incentive uptake.

Insurer and broker representation should be formalised within Horizon 2 governance structures (e.g. the Executive Cyber Council) to ensure continuous feedback loops between policy design, market behaviour, and sector outcomes.

- Include SME/NFP representation in any cyber-insurance working group to keep affordability and accessibility central to design

Replicate successful public-private models (e.g. terrorism pools) to structure systemic risk governance.

- This would replicate successful public-private governance models used in other critical risk domains (e.g. terrorism insurance pools).

HORIZON 2 – SHIELD 1 STRONG BUSINESS AND CITIZENS Non-Legislative Levers

3. Shield-level focus for Horizon 2 - 3.1 Shield 1: Strong businesses and citizens

Questions 5 through 11

Insurance Industry participation and role

Levers include threat-sharing platforms, voluntary standards, workforce grants, procurement incentives, threat exercises, and incident response frameworks.

Section	Lockton Position & Proposals
Strategic Alignment	Cyber insurance fosters risk-based cyber maturity uplift across sectors; Horizon 2 should explicitly integrate insurance ecosystems into threat-shield and SME support mechanisms.
Insurance Enablement Pilots	Commonwealth–industry pilots delivering co-funded maturity assessments to SMEs, with premium subsidies and optional insurer-led mentoring.
Maturity Frameworks & Standards	Advocate for modular maturity frameworks (e.g. based on ACSC Essential Eight or ISO 27001 Lite) with multi-tier certification recognised by insurers.
Threat Intelligence Integration	Enable legal and technical pathways for insurers to anonymised-share loss data with ACSC/ASD; promote underwriting insight as input to threat-sharing platforms.
Workforce & Accreditation	Government to support development of accredited training schemes for cyber insurance brokers & advisers; joint cadetships with Lockton and others.

1. Strong businesses and citizens

Overview

How Can Australia:	Lockton Proposed Course of Action
Consolidate our cyber awareness messages across the economy?	ACSC awareness update to include an "Insurance & Resilience" insert
Increase cyber literacy in our schools and early learning programs?	ACARA micro-unit on risk pooling/insurance within Civics/Economics
Target resilience uplift to small and medium-sized entities that cannot adequately protect themselves, including through tailored cyber security standards that are cheap to apply?	Cyber Uplift Voucher pilots (two sectors; co-funded assessments + controls + insurance readiness) Insurer-aligned SME/NFP baseline. Introduce tiered maturity-linked insurance incentives. (8–10 controls; one-page attestation)
Enhance support for citizens and victims of cybercrime to help them bounce back quicker?	Support victims of ransomware and identity crime by leveraging insurer-provided 24/7 incident response panels. Identity Restoration Pathway via insurer panels for citizens affected by insured SME/NFP breaches
Harmonise and simplify cyber regulation to promote best practice and efficiency?	Harmonised thresholds & safe harbour aligned to insurance triggers
<u>Insurance specific:</u> Do you consider cyber insurance products to be affordable and accessible, particularly for SMBs? If not, what factors are holding back uptake of cyber insurance?	Update ACSC awareness assets to include a one-page "Insurance & Resilience" insert (co-badged with industry) Short-Form SME/NFP proposal pack endorsed by local insurers Two-year premium support pilots tied to verified control adoption and outcomes.

Detail

Risk-Based Maturity Uplift Through Insurance Enablement

Insurance design is dynamic and can be harnessed for cyber maturity evolution. Ultimately, insurance lowers systemic distress risk, which is aligned with government's goal of national economic resilience.

Q1. How can Australia consolidate cyber awareness messages across the economy?

Lockton response

- Use government channels to explicitly recognise the role of cyber insurance in resilience messaging, alongside the ACSC Essential Eight and SMB1001, so organisations see insurance and controls as complementary.
- Publish plain-English myth-busters (e.g., "cyber insurance doesn't pay") and direct SMEs/NFPs to a short *How insurance responds* explainer (first-party, third-party, and incident-response benefits) aligned to ACSC guidance.

Action (Government)

Update ACSC awareness assets to include a one-page "Insurance & Resilience" insert (co-badged with industry) within 3 months.

Example Measure

≥100k downloads in year 1; ≥70% recall in SME/NFP pulse survey.

Q2. How can Australia increase cyber literacy in schools and early learning?

Lockton response

Introduce a simple "risk & resilience" module (digital safety + how insurance pools risk) within Year 9–10 commerce/digital tech curriculum, linking cyber hygiene to real-world recovery and community resilience.

Action (Government + Education):

Commission ACARA to embed a micro-unit on digital risk pooling/insurance within the relevant curriculum pilot within 12 months.

Example Measure

Pilot in ≥200 schools; pre/post literacy delta ≥15%.

Q3. How do we target uplift for SMEs and NFPs that cannot adequately protect themselves, including cheap tailored standards?

Lockton response

- Pair Essential Eight/SMB1001 "lite" baselines with insurer-recognised checklists (MFA, EDR, patching cadence, IR plan testing). (elaborated page 20).
- Use insurance-linked incentives to reward incremental uplift (tiered premiums/coverage breadth), so smaller entities can enter the market and improve over time.
- Provide access to insurer/broker panel response so SMEs/NFPs can "rent" expertise they cannot staff internally.

Action (Government + Industry)

Launch a Cyber Uplift Voucher (co-funded maturity assessments tied to controls adoption and insurance readiness) in two priority sectors within 6 months.

Government–market pilot programs

- A Commonwealth-funded pilot could provide matched funding for insurer/broker-delivered maturity assessments, with premium subsidies for entities implementing agreed remediation measures.

Publish an insurer-aligned SME/NFP baseline (8–10 controls mapped to Essential Eight/SMB1001) with a one-page attestation template (see appendix page 20).

Example Measure

5,000 SMEs/NFPs complete attestation in year 1; ≥40% obtain/renew cover at improved terms.

Q4. How do we enhance support for citizens and victims (ransomware, identity crime) to bounce back quicker?

Lockton response

- Leverage insurers' 24/7 panel services (IR, legal, PR, forensics) which are frequently engaged below deductibles, accelerating containment and recovery.
- For identity crime, provide co-funded restoration services via insurers' panel providers (credit monitoring, document replacement guidance) for affected citizens of insured NFPs/SMEs.

Action (Government + Insurers)

Establish an Identity Restoration Pathway that directs insured entities' customers to panel services within 48 hours post-breach.

Example Measure

Median time-to-notify ≤72 hours; identity restoration initiated ≤7 days in ≥xx% of cases.

Q5. How do we harmonise and simplify cyber regulation to promote best practice and efficiency?

Lockton response

- Align incident thresholds and timelines across SOCI, Privacy Act and proposed ransomware reporting with common insurance notification norms to remove duplication and confusion.
- Expand safe harbour for entities meeting insurer-recognised baselines (reduced penalties/streamlined reporting), encouraging uptake without heavy-handed mandates.

Action (Government)

Publish a single reporting threshold table cross-walking SOCI/Privacy/ransomware with insurer triggers; implement safe harbour via rules within 12 months.

Example Measure

TBD

More broadly

Risk-based incentives for maturity uplift

- Formalise insurance as a mechanism for achieving cyber maturity targets by linking premium advantages, coverage breadth, and limit availability to verifiable security controls (e.g. ACSC Essential Eight maturity, ISO 27001, NIST CSF).
    - i.e., Insurance as an enabler, not merely a compliance tick box:
- Incentives should be tiered - rewarding incremental uplift to encourage participation from entities at varying maturity levels, especially SMEs and regional operators.
    - Insurers can design tiered cyber insurance programs that reward demonstrable cyber hygiene (e.g. CERT aligned protocols, regular tabletop testing, incident response plans). This approach aligns with risk based maturity uplift across all sectors, particularly SMEs.

Example Measure

TBD

Specific Cyber Insurance question

The role of cyber insurance in strengthening cyber resilience for businesses and NFPs

Do you consider cyber insurance products to be affordable and accessible, particularly for SMBs? If not, what factors are holding back uptake of cyber insurance?

Executive Summary Response

Summary

Cyber insurance is a practical mechanism for improving cyber resilience at the entity level (access to capital, response capability, and continuity) and the economy level (reduced distress, preserved jobs, and faster recovery).

It complements - not replaces - cyber security investment: controls reduce the frequency of incidents; insurance reduces their financial and operational severity, creating a whole-of-event safety net (prevention up front; protection and recovery after).

When embedded into national settings, insurance incentivises uplift (minimum standards), enables access to expert response services (often below deductibles), and provides data-driven insight on the controls that most reduce loss.

What factors are holding back uptake of cyber insurance

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.

We further believe there to be a variety of reasons for this widening protection gap for SMEs, including believing that cybersecurity is "too hard" and they are "too small to target", they face more immediate pressures, and cyber insurance is still relatively new, with questions around coverage, cost and value, per the points raised above.

In practice, well-structured cyber insurance policies do pay, and insurers are paying out 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.
- Time-limited, co-funded pilots that pair control adoption with premium support (vouchers) and broker-delivered readiness assessments.
- Standardised SME/NFP proposal set (short-form, insurer-endorsed) to reduce friction.
- Myth-busting and case studies published jointly by Government and industry.

Action

Create a Short-Form SME/NFP Proposal Pack (≤25 questions, mapped to Essential Eight/SMB1001) endorsed by a consortium of local insurers within 6 months.

Fund two-year SME/NFP Premium Support Pilots (co-funding capped, tied to verified control adoption and claims learning).

Example Measures

Bound-policy conversion rate +25%; average premium change ≤CPI for pilot participants; ≥20% reduction in quote-to-bind cycle time.

Detailed Answer

1. Key Challenges in Selling or Buying Cyber Insurance

Insurance misconceptions - "Cyber Insurance doesn't pay"

Overview

- A persistent perception exists that "cyber insurance doesn't pay". In reality, standalone cyber policies pay valid claims at very high rates:
    - In 2024, Australian insurers paid approx. AUD $247m in cyber claims.
    - In the US, insurers paid USD $4.3bn in claims in 2022 (44.6% of all cyber premium collected).
    - CFC, a leading global insurer, reported paying 99.1% of cyber claims.
- Media bias exacerbates this, with most reported disputes concerning war exclusions under traditional policies (e.g., Mondelez case), not standalone cyber policies.

Detail

The perception that cyber insurance doesn't respond to claims is often due to misunderstandings about policy coverage and claim procedures, or, an albeit rare, poor claims experience.

In reality, when policies are well-structured and aligned with the organisation's risk profile, insurers do pay out valid claims. For example, in 2024, Australian insurers paid approximately AUD $247 million in cyber claims, reflecting the industry's responsiveness to legitimate incidents. (elaborated page 24).

Further, CFC - one of the world's leading cyber insurers - recently disclosed that it paid 99.1% of all cyber insurance claims submitted, reinforcing when policies are structured correctly and aligned to organisation risk profile, insurers do respond.

The myth that "cyber insurance doesn't pay" is largely fuelled by a small number of disputes under traditional policies not designed to cover cyber losses, rather than standalone cyber policies, or those with ulterior motive.

b. Confusion with Conventional Insurance

Overview

- Many cyber event related coverage "disputes" arise under general liability, property, or all-risks policies. Customers relying on these products are often disappointed when cyber exposures are excluded - reinforcing misconceptions.

Detail

There is an awareness gap, with business leaders (particularly SMEs/NFPs) often having limited knowledge of what cyber insurance covers or how to align posture with insurer expectations.

Beyond the obvious and clear story told by the data, peer reviewed research also assists in dispelling the above false non-payment rhetoric. "Investigating online reporting on insurance disputes over cyber losses" (Daniel Woods, et al.) found that very few "cyber insurance" related disputes actually relate to standalone cyber insurance. Out of 101 media and legal articles reviewed, only 5% referenced disputes with cyber-specific policies. Most disputes stemmed from claims under traditional policies (e.g. liability, property, all-risks), where cyber losses were not intended to be covered - leading to unmet expectations.

The study also highlighted a reporting bias: mainstream media disproportionately focused on "war clause" disputes, with 19 of 20 references tied to just two high-profile cases. Yet, notably, there were no reported war clause disputes involving standalone cyber policies, creating a misleading perception that such exclusions are commonly used to deny cyber claims.

The majority of disputes are related to claims under traditional policies, such as commercial general liability, all-risks and property policies, (i.e., the Mondelez case).

c. The "Prevention vs Insurance" False Choice

Overview

- IT/security professionals sometimes position insurance as unnecessary, promoting security controls alone.
- This ignores the reality that controls shrink risk but don't eliminate it, while insurance provides capital and response support for residual risks. The two are complementary, not substitutes.

Detail

Two sides of the same coin

Investment in cybersecurity shrinks, but does not eliminate risk, and cyber insurance mitigates the risk organisations cannot eliminate, or predict.

Investment in cyber security controls is non-negotiable. Strong governance, technical defences, and awareness programs shrink an organisation's exposure and build resilience. However, no level of investment can eliminate cyber risk entirely. Zero-day vulnerabilities, supply chain failures, insider threats, and state-sponsored activity remain outside the control of even the most mature enterprises.

This is where cyber insurance plays a complementary role. It mitigates the unpredictable, unpreventable, and catastrophic exposures that cannot be fully controlled through internal investment alone. By transferring residual risk off the balance sheet, insurance ensures continuity, access to capital, and structured recovery support.

Complementary, not competing

Cyber security spend and cyber insurance should not be viewed as substitutes. Controls reduce the frequency of incidents; insurance reduces the severity of their impact. Together, they provide a whole-of-event safety net: prevention on the front end, protection and recovery on the back end.

For example, insurers analyse thousands of claims to identify which controls most effectively reduce loss frequency (e.g. MFA, EDR, backup segmentation). Organisations benefit twice:

1. From direct investment in those controls; and
2. From the premium, coverage, and incident response advantages insurers extend when those controls are in place.

In short: cyber security investment reduces the likelihood of an incident, cyber insurance reduces the cost when incidents inevitably occur. Together, they create a virtuous cycle that makes organisations, individuals, and the economy stronger.

d. Minimum Standards and Complexity

Overview

- Insurers are raising "the floor" of required controls (MFA, EDR, patching, IR plans). While positive, SMEs and NFPs often struggle with cost and resource capacity to meet these standards.
- The result is the perception that cyber insurance is "hard to get" or unaffordable.
- The reality is that insurance standards very much align with best in class broader cybersecurity standards.

Detail

Insurers are increasingly raising the floor of cyber security requirements, with controls such as multi-factor authentication (MFA), endpoint detection and response (EDR), timely patching, and tested incident response and continuity plans now expected as standard.

These baselines are informed by extensive claims data, which consistently shows that these measures most effectively reduce loss frequency and severity. While this is a positive driver of national uplift, many SMEs struggle with the costs and resources needed to meet these requirements, fuelling the perception that cyber insurance is "hard to get" or unaffordable.

The reality, however, is that insurer expectations closely align with existing best-practice frameworks, including the ASD Essential Eight and SMB1001, particularly around patching, privileged access management, MFA, and secure configuration. In some areas - such as continuous monitoring, staff training, and tested incident response plans - insurers even go further, reinforcing resilience gaps not always captured in technical baselines.

This demonstrates that cyber insurance does not create artificial barriers; rather, it drives alignment with national cyber standards and ensures organisations focus investment on the most impactful controls.

What Government Could Do

Lockton recommends the Government support adoption by:

- Education and myth-busting

  Publicly affirm that cyber insurance does pay claims, using ASIC/ACSC/industry data to demonstrate responsiveness.

  Create a Short-Form SME/NFP Proposal Pack (≤25 questions, mapped to Essential Eight/SMB1001) endorsed by a consortium of local insurers within 6 months.

- SME incentives

  Support pilots co-funding cyber insurance premiums linked to posture improvements (similar to energy efficiency or OH&S programs).

- Safe harbours

  Offer regulatory relief or reduced penalties for entities holding cyber insurance and meeting agreed benchmarks.

- Procurement levers

  Require suppliers to hold cyber insurance as evidence of maturity, stimulating broader uptake.

- Threat-sharing integration

  Formally embed insurers into ACSC/ASD threat-sharing ecosystems to amplify their role as "proxy regulators".

Summary

Cyber insurance penetration is held back not by lack of value, but by misconceptions, awareness gaps, and SME affordability constraints. Government recognition of its benefits, coupled with targeted incentives and insurer integration into policy frameworks, will accelerate adoption and uplift national resilience.

Conclusion

Horizon 2 offers an inflection point to move from foundational reforms to scaled, sustainable maturity uplift.

Lockton Australia stands ready to partner with government, insurers, and industry in designing programs that blend policy ambition with market pragmatism, leveraging insurance as a driver of resilience, competitiveness, and trust.

Annexure

Cybersecurity Control Alignment

Cyber Insurance vs SMB1001 vs ASD Essential 8

Below, is a structured matrix comparing and aligning a consolidated, broadly market aligned Cyber Insurance industry control posture expectations with SMB1001 and the Australian Signals Directorate's (ASD) Essential Eight: This comparison is intended to clarify areas where cyber insurance posture requirements intersect with key Australian standards.

Areas of Alignment

Areas of strongest alignment include Patching, Privileged Access Management (PAM) and Multi-Factor Authentication (MFA), consistently emphasised across cyber insurance requirements, SMB1001, and Essential Eight:

Areas of Notable Misalignment or Gaps

1. **Continuous Monitoring – Gap identified**

Essential Eight does not explicitly include continuous monitoring as a requirement, creating a notable gap compared to cyber insurance expectations and SMB1001.

2. **Staff Training, Awareness and Testing – Gap identified**

Essential Eight does not explicitly require staff awareness training, whereas cyber insurers and SMB1001 explicitly include it as a core component of security posture.

3. **Testing of Incident Response & BCP/DRP – Partial Gap identified**

Essential Eight addresses backups as a resilience measure but does not explicitly require regular testing of incident response plans, business continuity plans, or disaster recovery plans, unlike cyber insurers and SMB1001.

Other Observations & Considerations

- While the Essential Eight is very technical and focused explicitly on mitigating cyber intrusion techniques, SMB1001 and cyber insurance controls are broader and include governance, monitoring, and preparedness controls.
- Cyber insurers place additional emphasis on operational readiness (Incident Response, Business Continuity, Disaster Recovery) and user awareness, areas less explicitly covered in Essential Eight but clearly highlighted within SMB1001.

Recommendations

Organisations aiming for comprehensive coverage can effectively combine all frameworks given the significant crossover, and address the Essential Eight as a technical baseline whilst proactively managing:

- Continuous security monitoring and logging practices,
- Staff awareness and regular training, and
- Formalised and tested Incident Response and Business Continuity Plans.

This combination fully aligns with cyber insurance expectations and broader ACSC guidance (SMB1001), ensuring enhanced cyber resilience and optimal cyber insurance underwriting outcomes.

With the above recommendation in mind, Lockton would like to support the Government in communicating an Insurance baseline alongside some leading insurers within Australia.

Cyber Insurance Control Requirements	SMB1001 Control Requirements	ASD Essential Eight Control Requirements	Commentary & Gaps
Reflects insurer preferences driven by underwriting criteria and claims experience, aimed at mitigating frequent or severe loss scenarios.	*Guidance for SME's provided by Cyber Security Certification Australia (CSCAU), focusing on essential, manageable security controls.*	*Core mitigation strategies recommended by the ACSC, aimed at protecting organisations from cyber threats, notably ransomware and malware*	Alignment, gaps and context (where relevant).
Patching within limited timeframe of release	Timely Patching & Updates **Strong Alignment**	Patch Applications, Patch Operating Systems **Strong Alignment**	Strong alignment. All frameworks prioritise prompt patching as a critical defensive measure against vulnerabilities.
Tightening web security settings	Secure Configuration & Web Protections **Strong Alignment**	Application Control, Restrict Administrative Privileges **Partial Alignment**	Good alignment with SMB1001, covering web configurations. However, Essential Eight does not explicitly target general web settings. It focuses more specifically on application execution controls, macros, and privileges rather than broad web security.
Ensuring privileged access management controls are in place	Access Management & Control) **Strong Alignment**	Restrict Administrative Privileges **Strong Alignment**	Strong alignment. All frameworks agree strongly on privileged access management as a fundamental cybersecurity control.
Conducting continuous monitoring of events and infrastructure	Logging and Monitoring **Strong Alignment**	Not explicitly covered in Essential Eight **Limited Alignment**	Misalignment noted. Cyber insurance and SMB1001 explicitly recommend robust logging and monitoring practices, whereas Essential Eight does not explicitly require continuous monitoring. Essential Eight focuses more on preventive over detective controls.
Applying hardening techniques across systems and settings	Secure Configuration **Strong Alignment**	Application Control, User Application Hardening, Configure Macro Settings **Strong Alignment**	Strong alignment. Cyber insurance control is broader, covering general system hardening, while Essential Eight explicitly mentions specific types of application and macro hardening. SMB1001 explicitly covers secure system configuration practices.
Staff Training, Awareness and Testing	Staff Awareness & Education **Strong Alignment**	Not explicitly included in Essential Eight **Limited Alignment**	Misalignment noted. Cyber insurance explicitly calls for staff training, awareness, and regular testing. SMB1001 aligns explicitly. Essential Eight, however, does not directly address staff training and assumes organisational knowledge or separate ACSC/ASD guidance covers this aspect.
Testing of IRPs, BCPs and DRPs	Incident Response & Business Continuity Plans **Strong Alignment**	Indirectly through Regular Backups **Partial Alignment**	Partial alignment. Cyber insurance and SMB1001 explicitly prioritise incident response, business continuity, and disaster recovery planning/testing. Essential Eight indirectly supports this through backup strategies but lacks explicit emphasis on incident response and BCP/DRP testing.

MFA implementation across specific areas	Multi-Factor Authentication **Strong Alignment**	Multi-Factor Authentication **Strong Alignment**	Strong alignment across all frameworks. Multi-Factor Authentication is universally recognised as a foundational control.

Cyber Insurance – Context and position as an enabler – Detail

Value & Context of Risk Transfer – Empowering Organisations

There is a cost to bearing organisation-specific risk, and a value to controlling such risk. Additionally, organisations with more growth opportunities will value retained capital more and will benefit from protecting it through risk management and risk transfer (insurance), even at a cost to current earnings (i.e., paying premiums).

Further it can be argued that risk reduction, specifically via insurance can actually enhance earnings. Simply, if it costs something to reduce risk (i.e., protecting profit, or adding confidence to customers, or meeting contractual requirements), but higher earnings result, then risk management and transfer, adds to value.

The case for capital allocation to premiums

Allocating capital strategically into enhanced risk protection (i.e., increasing existing liability limits or extend coverage to previously uninsured risk areas) offers more substantial, long-term value to Australian organisations.

This proactive approach not only fortifies organisation's risk resilience but also ensures preparedness against potential future losses or liabilities that could significantly surpass the retained savings.

Investing capital in risk transfer (insurance) provides enhanced financial predictability by mitigating potentially severe and unplanned costs arising from catastrophic events or unforeseen exposures, also supporting stable financial management and capital optimisation by reducing volatility and safeguarding retained earnings.

Finally, targeted reallocation positions organisations more favourably in the eyes of key stakeholders - including regulators, customers, suppliers, and investors - reinforcing your reputation as a resilient and proactive-thinking organisation. Deliberate reallocation of premium savings into strengthening your risk management posture represents a strategic investment, offering meaningful financial security, operational stability, and stakeholder confidence beyond short-term benefits of retaining these savings alone.

Directors Duties

Additionally, an appropriately implemented Insurance program has an equally important role to play in directors' and officers' meeting their duties. Transferring risk to the insurance market, assists in demonstrating prudent governance of organisational risk, helping mitigate directors' and officers' exposures.

Directors are responsible for creating and maintaining cyber resilient enterprises, and failing to do so brings significant potential personal liability.

Cyber Insurance's relevance in a Cyber Event

In a catastrophic cyber event, management often have no choice but to focus on the immediate issues of distress, taking time and energy away from pursuing strategic value. These broader costs start to impact organisations well before the often first thought of concern of insolvency of which the mere prospect of may trigger employees, suppliers, and customers to begin looking elsewhere.

Further, distress unambiguously impacts funding (if relevant). Once in distress, organisations find it hard to raise outside funds, and virtually impossible to raise external equity capital, with those reticent to "throw good money after bad."

These two features of distress associated with catastrophic events – higher costs and reduced financing opportunities - make it a death spiral from which exit is very difficult.

As a result, the prospect of distress, even if distant, should be built into everyday values around risk management, as risk management can raise every-day value, primarily by reducing the probability of distress or near-distress states.

Value & Context Of Risk Transfer – Economy Perspective

Overview

Risk management isn't just about avoiding negative outcomes and is not just about individuals. It can also be the catalyst that drives organisation and economic innovation and growth. Risks are inevitable for organisations, and countries to innovate and remain competitive. Competitive risk is a challenge that must be constantly monitored and address.

Enabling growth, enabling the economy

Any organisation, and economy operating in a competitive market must focus its attention on changes in the external environment that could impair its ability to create value for its customers, or in creating a competitive economy. To do so, takes significant time and resourcing. This requirement to define and communicate risks to avoid - especially from a whole of economy standpoint - is essential to ensure risks don't extinguish innovation. Australia's business history shows that good risk management doesn't stifle innovation - it enables it. Firms that treat risk as a strategic asset, not just a compliance burden, have consistently outperformed.

- Macquarie Group built a global investment powerhouse on the back of a robust risk management framework. Its ability to anticipate and manage shocks gave leadership the confidence to enter new markets and scale globally.
- SafetyCulture turned risk management into a growth engine, digitising safety checklists into a platform now used by millions. By embedding risk into daily workflows, they unlocked new business models.
- Optalert transformed fatigue risk into innovation by building a wearable monitoring system now adopted by transport and mining giants, enhancing both safety and operational continuity.

These stories demonstrate that when risk is well-informed, well-managed, and well-insured, it inspires confidence - for boards, investors, customers, and regulators. Cyber insurance is therefore not a brake on ambition, but a springboard for growth - turning threats into opportunities and helping position Australia as a resilient digital economy leader under Horizon 2.

Insurance Market Statistics/Loss Ratios – Context

~$28M IN CYBER CLAIMS PAID BY APRA REGULATED INSURERS LAST QUARTER

The often-privileged (LPP) nature of events can make claims data somewhat difficult to source, however APRA has commenced including Cyber Insurance Loss data in their Quarterly general insurance performance statistics (now coming into its 5th quarter reporting period). APRA authorised insurers have somewhat consistently sat at a ~50-60% gross loss ratio per quarter.

Over the last 3 years we have observed loss ratios range from 30% to 90% for established Cyber Insurance portfolios, demonstrating the volatility of claims experience particularly if exposed to large losses. Overall, we estimate that the underlying gross of reinsurance loss ratio for Cyber is —55%, with SME Cyber around and Mid-Market/Corporate Cyber running higher at around 60-80%.

Cyber

Quarter ended ($ million)	Dec 2023	Mar 2024	Jun 2024	Sep 2024	Dec 2024
Gross written premium	73	42	53	39	70
Number of risks written ('000s)	24	7	7	4	3
Insurance revenue	52	51	41	46	47
Insurance service expense	-34	-33	-25	-16	-28
Incurred claims	-54	-29	-14	-28	-19
Other insurance service expenses	*	-2	*	-1	-5
Amortisation of insurance acquisition cash flows	*	-6	-6	-6	-6
Losses and reversal of losses on onerous contracts	0	0	0	*	*
Changes that relate to past service: Changes to liabilities for incurred claims	31	4	-2	20	2
Impairment losses/reversals on assets for insurance acquisition cash flows	0	0	*	*	*
Insurance service result before reinsurance contracts held	19	18	17	30	19
Allocation of reinsurance premiums	-28	-27	-21	-25	-26
Amounts recoverable from reinsurers	28	4	18	13	12
Net expense from reinsurance contracts held	0	-24	-3	-12	-14
Insurance service result	18	-6	14	18	5
Average premium per risk ($)	3,082	6,213	7,173	8,821	22,934
Cession ratio	53.3%	53.7%	50.1%	54.7%	54.8%
Gross loss ratio	42.9%	49.9%	41.0%	*	*
Net loss ratio	-22.1%	92.3%	-5.6%	*	*
Net combined ratio	24.8%	124.9%	32.0%	11.9%	75.5%

Source: https://www.apra.gov.au/quarterly-general-insurance-performance-statistics

$4B
2025 GLOBAL REVENUE

13,100+
ASSOCIATES WORLDWIDE

65,000+
CLIENTS WORLDWIDE

155+
COUNTRIES REPRESENTED

94%
CLIENT RETENTION

13%
ORGANIC GLOBAL GROWTH

$20M+
COMMUNITY IMPACT

Lockton Australia – Technology Sector Practice

Lockton Australia is the only broker that can provide the comfort and security of a major international broker, the highest levels of service and client centricity, and the specialism of Australia's leading Technology Sector Practice.

TECHNOLOGY SECTOR SPECIALISTS

With expertise in delivering ongoing risk advisory and insurance placement services for examples like Australia's Largest Cloud-based Health Data Project solution, to the ASX's largest Tech Sector listing in 2024, our Technology Sector Practice has the specialism, strength, scale and innovative perspective to deliver your risk advisory and insurance objectives.

INFORM – IMPROVE – INSURE

Our focus on the Technology Sector permeates across all facets of risk in technology, data, property, people and liability, and is underpinned by our holistic Inform, Improve, Insure approach to risk advisory and insurance placement services.

BEYOND BROKING EXPERTISE

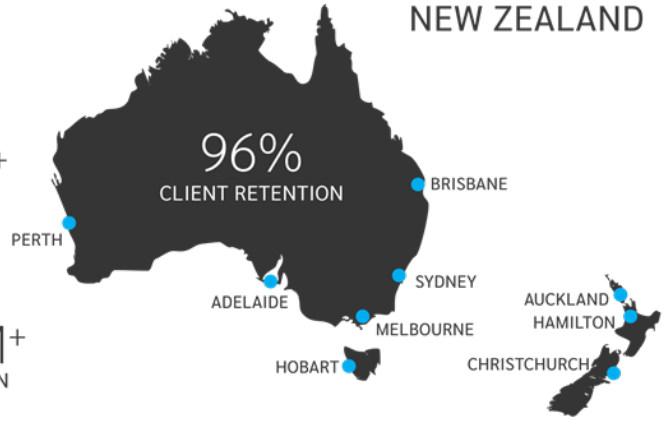
Beyond our client specific and insurance wording/cover expertise, our broader sector involvement sets us apart, including partnerships with key industry and government bodies.

Partnerships and work with the Tech Council of Australia (TCA) and the National Office of Cyber Security facilitates meaningful Tech Sector policy contributions and value for our clients.

340+
ASSOCIATES

4,200+
CLIENTS

$958M+
GROSS WRITTEN PREMIUM
into insurance market



Great Place To Work. Certified APR 2024-APR 2025 AUS

Great Place To Work. Certified APR 2024-APR 2025 NZ

Best Workplaces for Women Great Place To Work. AUSTRALIA 2023

From start up to scale up to established tech, we specialise in working with Tech Sector organisation of any size that innovate, design, develop, manufacture, supply, or support technology products or services.

Development of bespoke Tech Sector specific coverage solutions like our proprietary Hich Compliance+ Tech E&O/Cyber wording.

Significant claims experience from technology sector contract disputes to ransomware negotiations, involving engagement with the ACSC.

Ongoing Sector contributions via speaking engagements with associations like AISA, AILA and other sector specific bodies and associations.

Our Mission

To be the worldwide value and service leader in insurance brokerage, risk management, people solutions and retirement services.

Our Goal

To be the best place to do business and to work.

ADELAIDE | BRISBANE | HOBART | MELBOURNE | PERTH | SYDNEY

Lockton Companies Australia Pty Ltd
(ABN 85 114 565 785 / AFSL 291 954)
global.lockton.com

LOCKTON®