Australian Cyber Security Strategy: Legislative Reforms

Consultation Paper

March 2024

Property Exchange Australia Limited | Level 16, Tower 4, 727 Collins Street, Docklands VIC 3008

Document and contacts

Document Title:
PEXA’s Australian Cyber Security Strategy: Legislative Reforms response

Document date:
March 2024

Contact for inquiries:

David Willett
Chief Information Security Officer

Damien Manuel
General Manager, Regulatory Affairs

Marko Jovanovic
Privacy Officer

Tower 4, Level 16, 727 Collins Street
Docklands VIC 3008
Proudly located on Wurundjeri Country

T (+61) 03 7002 4500
W www.pexa.com.au

Contents

Executive Summary

PEXA is a world-leading ASX-listed digital property exchange platform and property insights solutions business. PEXA was formed in 2010 to fulfil the Council of Australian Governments' (COAG) ambition to deliver a single, national e-conveyancing solution to the Australian property industry. This ambition is very close to being realised, with six of Australia's eight jurisdictions now digitally integrated for e-conveyancing. Since 2013, PEXA has facilitated more than 16 million property settlements through the PEXA Exchange in Australia, with 89% market reach. Having revolutionised property transactions in Australia, the PEXA Group of digital businesses, including .id (Informed Decisions), Value Australia, and Land Insights, is now delivering innovative, data-driven property solutions that help government, financial institutions, banks, and property practitioners unlock the future value of property.

As a provider of critical services to the Australian economy, PEXA recognises the importance of cyber security legislative reform and other amendments to the SOCI Act. The evolving and changing threat landscape means continual monitoring and adjustment to settings that promote and ensure the safety of Australian citizens and businesses will be required.

PEXA's response to all the measures proposed in the consultation paper can be summarised by the following three high level themes.

Theme 1: Striking a balance to enhance Australia's cyber resilience

1. Emphasis on proportionality: Any proposed reporting obligations should be proportionate to the scale of the threat, size/sophistication of the business and the flow on impacts to other businesses or the Australian economy. Overly prescriptive requirements may create unnecessary administrative burdens, disincentivise proactive cyber defence practices and may not be appropriate (i.e. one size does not fit all).
2. Focus on outcomes: Instead of imposing specific practices, consider defining expected outcomes that allow businesses the freedom to devise strategies for improved security while providing guidance based on practical real-world examples. This approach promotes innovation and adaptability, empowering businesses to take control of their cyber defence while also uplifting awareness and education.
3. Incentives and support: The government should be clearer on what support is available. This could encompass technical resources, tools, cyber security training, and information-sharing mechanisms. By doing so, reporting and learning from incidents becomes a joint effort for shared advantage, fostering engagement and collaboration.
4. Maturity assessment: Understanding the maturity of various sectors and how they could all work together. While some sectors have had the last 20+ years to mature, some relatively new CI sectors are struggling with attracting talent, resourcing (e.g.

funding and suitable technological solutions) and competing sector specific priorities (e.g. healthcare/medical and higher education/research).

Theme 2: Equity in Cyber Security

5. Tiered approach: A potential tiered approach could tailor reporting requirements to the scale and complexity of the organisation. This could involve simplified reporting for smaller businesses and more detailed, in-depth reports for Critical Infrastructure sectors.
6. Accessibility: Businesses of all sizes must quickly understand and implement the reporting process. This includes clear guidelines, readily available resources, and designated contact points for support.
7. Protecting sensitive information: Incorporating robust privacy safeguards within the reporting system is crucial. This includes transparent data collection, handling, and sharing guidelines to reassure businesses that sensitive information is secure and will not lead to unforeseen repercussions.
8. Education in cyber security within the government: The government must be forthcoming with lessons learned from past cyber incidents. This should include publishing use cases that provide intelligence to organisations that could be targeted based on recent cyber-attack patterns. Case studies should be accessible by business executives to better understand the business consequences, but also contain sections relevant for technical teams to protect their organisations.

Theme 3: Discouraging complacency and non-disclosure

9. Culture of shared responsibility: Emphasise that reporting is not a punitive measure but part of a national effort to combat cyber-crime. The importance of transparency needs to be communicated, demonstrating that the data is used to understand threat patterns better and enhance everyone's security.
10. Anonymisation and aggregation: Where possible, anonymised and aggregated data should be standard practice. This protects businesses and fosters broader trends analysis, benefiting the overall cyber security landscape.
11. No substitute for proactive defence: Reporting obligations should be clearly framed as an addition to robust defence strategies. No business should expect that reporting absolves them from the fundamental responsibility of solid cyber security.

Response to measures: Part 1 – New cyber security legislation

Measure 1: Helping prevent cyber incidents – Secure-by-design standards for Internet of Things devices

1. Who in the smart device supply chain should be responsible for complying with a proposed mandatory cyber security standard?

   PEXA’s view is that all parties have some level of responsibility to help prevent cyber incidents related to Internet of Things (IoT) devices. The Federal Government has the responsibility to protect consumers by ensuring appropriate legislative instruments, frameworks and guidance are established to ensure safe and secure IoT devices for businesses and citizens.

   Manufacturers selling IoT devices into the Australian market should ensure their devices have been designed with security in mind. A baseline standard should be adopted for initially consumer devices (AS ETSI EN 303 645:2023) and then at a later point, commercial IoT devices should be included once an international standard has been defined. It may be in Australia’s interest to work with the USA / UK and International Standard bodies to leverage elements of AS ETSI EN 303 645:2023 for commercial IoT devices (e.g. solar inverters, power systems, medical systems etc..).

   Consumers need to also take some responsibility for the devices they choose to buy and use. However, consumers often lack the awareness or sophistication to test and understand the security of consumer IoT devices. Consequently, consumers need a simple and easy to understand labelling mechanism which helps to inform consumers on the approximate safety / security of the IoT device they are purchasing. In some instances, changes to consumer law may be required to enable consumers to return insecure devices for a full refund to ensure a top down and bottom-up approach to force change and ensure more secure IoT consumer devices. This would require Home Affairs to work closely with ACCC to enable consumer protections in line with the mandatory cyber security standard.

2. Should a broad definition, subject to exceptions, be used to define the smart devices that are subject to an Australian mandatory standard? Should this be the same as the definition in the PTSI Act in the UK?

   The definition adopted by the Australian Government needs to be simple and easy for both consumers, new entrants to the Australian market and businesses to understand.

Rather than following the PTSI Act in the UK, the government should consider what is best in the Australian context. Is the legislation targeting consumer smart devices which is synonymous these days with any Internet connected device (e.g. smart phone, watch or speaker) or IoT consumer devices which are also Internet connected, but often associated with lower cost and lower processing power devices (e.g. sensors, temperature stations)? Maintaining a list of devices is insufficient as it would be time consuming to maintain and update. A set of clear and simple principles may be a better solution, however if designed incorrectly, it may inadvertently capture a broad range of devices the government may want to keep out of the legislation at this stage.

3. What types of smart devices should not be covered by a mandatory cyber security standard?

While it will be important for the government to balance the negative aspects of legislation and the consequential impact of manufacturers potentially withdrawing consumer options, due to our limited market size, we can still be a leader by signalling our intentions and building alignment with other countries. It is inevitable through the lack of a global standard that each country will implement their own reforms, resulting in a global patchwork of legislation. Historically we have seen this with the state of California often passing very forward leading legislation to protect consumers or the environment and provide certainty with regards to technology and how it is used. Due to the USA's market size, this often forces manufacturers to adopt the legislative change, which in turn encourages other countries to typically follow the USA and more specifically, California's lead.

Understanding that the Australian government is focused on consumer IoT devices termed smart devices (e.g. TV, watches, phones, speakers, toys), it should also strongly consider commercial IoT devices used in medicine, energy and other sectors to signal the shift to more security devices. Hence while legislation may be slowly or gently introduced for consumer devices with three baseline requirements, stating commercial devices will follow in a few years, will ensure manufactures and other countries take notice. The government should learn from the misstep with the voluntary IoT consumer code which manufacturers simply ignored. Therefore, the government now needs to legislate to create positive change. A similar thing should occur with commercial IoT devices as these devices create greater vulnerability points and threats for Australian businesses and the nation wholistically than consumer IoT devices.

A gradual step up of all IoT should be considered to ensure the risk is managed both for citizens and for Australian businesses. Just as we need to phase out combustible cars and our dependency on inefficient vehicles, we need to phase our poorly designed IoT devices which create weak points across the Australian economy.

4. **What is an appropriate timeframe for industry to adjust to new cyber security requirements for smart devices?**

A four-to-five-year grace period should be considered to allow for the following with regards to consumer smart devices:

- align with the expected life of devices, enabling consumers who have recently purchased a device to maximise the value of the investment.
- provide manufacturers with enough time to make necessary design or configuration changes in the production and packaging of new IoT devices.

While the legislative reform is primarily focused on consumer smart devices, it would be prudent for the Federal Government to signal to manufacturers that there will be requirements for industrial or commercial smart devices in the future to ensure these providers start to plan and factor in security improvements as they may require a five-to-ten-year lead time (e.g. medical devices, energy systems etc..).

5. **Does the Regulatory Powers Act provide a suitable framework for monitoring compliance and enforcement of a mandatory cyber security standard for IoT devices?**

The government may explore developing a bespoke code to support the Regulatory Powers Act, to ensure it can deliver the desired outcomes for all stakeholders and organisations. This code would act to support organisations better understand all potential implications associated with any mandatory standard.

Measure 2: Further understanding cyber incidents – Ransomware reporting for businesses

1. **What mandatory information, if any, should be reported if an entity has been subject to a ransomware or cyber extortion incident?**

The information collected should be pertinent to any investigation from a legal perspective. However, it should also be gathered to increase the broader Australian public's resilience to future attacks. The goal should be to collect intelligence that the Cyber Incident Review Board (CIRB) can disseminate to help other businesses increase protections against similar attack vectors. As such, PEXA believes the following information should be collected at a minimum:

- Any data exfiltrated that could be used to harm the Australian public. This could be from multiple perspectives, such as privacy, national security, or general health and safety.

- Whether any exfiltrated data was encrypted.
- Details of the ransom demand to determine motivation (financial or espionage). This can include how the ransom was received (email, etc.), the amount requested, and any information available on its source. Also, if the ransom is attributed to any group.
- Known information on the attack vector used. Whether this be a known software vulnerability, compromised credentials, resource misconfiguration, etc.
- Known information on variant(s) of ransomware or malware used to encrypt and/or exfiltrate data.
- Whether the incident has been mitigated. Or if there is still a persistent threat to the impacted business.
- Details of what measures have been taken to mitigate and prevent recurrence.

PEXA advises that ransomware incidents evolve quickly. An organisation will only be able to speak to the facts of what they know and should not be tempted to "speculate" as to what may/may not have happened.

2. What additional mandatory information should be reported if a payment is made?

The information requested should be focused on gathering further intelligence for law enforcement. Therefore, PEXA recommends providing the following if a ransom is paid.

- Justification for paying the ransom. Were lives or people's safety at risk? Or was there a risk to national security or the economy?
- Whether or not making the payment successfully restored access to encrypted data. Similarly, whether it prevented the release of stolen data. And if confirmation was received that stolen data was deleted.
- Time to receive decryption keys from time of payment (e.g. 24 hours, instantaneous, weeks etc..)
- Time to restore services post payment and post receipt of decryption keys.
- The amount paid to help understand the financial impact on the Australian economy and trends in cybercrime.
- The currency the payment was made in. If it was cryptocurrency, it is necessary to know what type and the recipient/wallet details. Regardless of the payment time, knowing this could be useful for tracing funds and potentially disrupting criminal networks if their preferred payment method is understood.
- When was the payment made to further aid in tracing efforts.
- Any communications with the ransomware attacker to help understand their techniques.

It would be essential to anonymise some of this information to protect the reporting organisation. If this were not to occur, it could result in follow-up attacks from other threat actors who know that the business in question has paid in the past.

Finally, the reporting method should not be so complex that it discourages reporting. Ideally, there should be a secure method to provide all details quickly and efficiently with the understanding that the complete picture may not be available straight away.

3. What is the appropriate scope of a ransomware reporting obligation to increase visibility of ransomware and cyber extortion threats whilst minimising the regulatory burden on entities with less capacity to fulfil these obligations?

   The government should take a pragmatic approach when an organisation reports ransomware. Depending on the immediate consequences to national security or public safety, a cadence should be established for notifying that an incident is confirmed and the type of mandatory information that will need to be ascertained over time. Providing a balance between allowing an organisation to work through the issue whilst not being too distracted by requests for information.

   The scope of obligations should be shared with regulators. This can enable standards to be built into existing regulatory frameworks instead of creating additional costs and overhead to comply with separate government standards.

4. Should the scope of the ransomware reporting obligation be limited to larger businesses, such as those with an annual turnover of more than $10 million per year?

   The proposal to set a standard on which organisations should report based on their annual revenue is sound. However, this may limit the threat intelligence the government can gather and share with the broader community. Instead, the government should consider the scope based on the impact of a ransomware attack and its consequences to the Australian public.

5. What is an appropriate time period to require reports to be provided after an entity experiences a ransomware or cyber extortion attack, or after an entity makes a payment?

   Determining the appropriate reporting for ransomware and extortion is a complex issue. Several factors influence reporting timeframes for organisations. This can include:

   - Urgency and Impact: Immediate knowledge of attacks helps facilitate timely law enforcement response, potentially limiting damage and stopping criminal activity.

- **Incident Assessment:** Businesses need time to assess the situation fully, understand the type of attack and potential data exposure, and gather the necessary information for an accurate report.
- **Operational Overhead:** Excessively tight deadlines can burden strained resources during an incident response.
- **Existing regulatory requirements:** This includes disclosure to shareholders for publicly listed companies. As well as mandatory notifications to regulators and other governing bodies.

PEXA believes it would be helpful to consider the following approaches.

- **Tiered Reporting:** Consider a tiered approach based on risk. This could mean critical infrastructure entities and incidents with significant potential harm must be reported within a shorter timeframe (e.g., 24-72 hours). Other organisations could have a slightly longer reporting window.
- **Initial Notification and Supplements:** Allow for an initial notification within a tight timeframe (e.g., 24 hours), indicating a suspected ransomware event. Follow this up with more detailed reports as the investigation progresses and information becomes available.
- **Payment-Focused Reporting:** A short timeframe (e.g., 24 hours) helps track criminal fund flows if payment has been made. However, organisations face considerable pressure from extortionists when a payment is demanded.
- **Aligned to Existing Regulatory Expectations:** The government should seek feedback from regulators and other governing bodies in the design of these requirements.

6. To what extent would the no-fault and no-liability principles provide more confidence for entities reporting a ransomware or cyber extortion incident?

Overall, no-fault and no-liability principles could significantly encourage more timely and comprehensive reporting of incidents. However, careful consideration and guidelines would need to be considered. This would be essential to fostering a collaborative environment for all stakeholders and enhancing Australia's cyber resilience.

PEXA can view the following positives from these principles.

- Putting the focus on solutions and not blame.
- Assisting organisations to mitigate reputational damage.
- Reassurances to businesses against retribution.

However, there are nuances to consider. The chances for such principles to create a culture where responsibility is not taken due to lack of repercussions is high. Therefore, PEXA advises taking care in considering the following when designing the principles.

- Scope of Protections: It's vital to define clearly what constitutes "no-fault" and "no-liability." Do they extend to cases of gross negligence, or do specific reporting standards still need to be upheld? Clarifying this avoids future misunderstandings.
- Balance with Accountability: Completely absolving businesses of any responsibility, even in cases of significant negligence, could undermine cyber security best practices. It's crucial to strike a balance where proactive defences are still encouraged alongside honest reporting.
- Public Perception: Shaping a public narrative on the purpose of incident reporting is vital. The message must be that reporting is a proactive step towards national cyber security, not a sign of weakness. Otherwise, some businesses might still hesitate, fearing public backlash.

.

7. How can the Government ensure that no-fault and no-liability principles balance public expectations that businesses should take accountability for their cyber security?

The government must consider its approach to designing, implementing, and enforcing these principles. As such, PEXA would recommend the following.

1) Defining Clear Scope and Purpose:
   - Situational Application: Develop explicit guidelines outlining when no-fault and no-liability protections apply. These should surround timely, good-faith reporting of ransomware or cyber extortion attacks for national threat assessment and consequence management.
   - Reinforcing Legal Due Diligence: Unambiguously state that these principles do not absolve organisations of their fundamental legal responsibility to implement reasonable cyber security measures. Companies must still diligently protect themselves and their customers' data.
   - Public Interest Focus: Position the no-fault and no-liability framework as a tool to enhance the Australian public's collective security. The emphasis should be on understanding the evolving threat landscape, not shielding businesses from the consequences of negligence.
2) Promoting Proactive Accountability:
   - Minimum Standards as Baseline: Establish industry-specific minimum cyber security standards to clearly define the basic level of protection expected as preconditions for no-fault/no-liability consideration.

- Collaborative Standards Development: Involve businesses, cyber security experts, and government agencies in developing and refining cyber security best practices. This shared ownership creates a sense of accountability within the private sector.

3) Emphasising Transparency and Shared Benefits:
   - Public Awareness Campaigns: Educate the public on the 'why' behind no-fault/no-liability principles. Honest reporting aids law enforcement efforts, helps businesses learn from each other, and ultimately benefits everyone through a more robust national cyber defence posture.
   - Data-Driven Guidance: Use aggregated, anonymised reporting data to guide targeted cyber security investments, sector-specific support, and public policy. This visible use of reporting insights builds trust.
   - Celebrating Successes: Publicize cases where reporting has led to the arrest of cybercriminals, the disruption of their operations, or the prevention of further attacks. This underscores the positive impact of responsible transparency.

8. What is an appropriate enforcement mechanism for a ransomware reporting obligation?

The Government should embrace a supportive and collaborative approach. This will create a culture where businesses may be more willing to report incidents. PEXA suggests the following to foster trust and maximise the value of threat intelligence shared to enhance Australia’s overall cyber resilience.

- Assistance-First Approach: The enforcement mechanism's primary function is facilitating timely reporting and encouraging widespread understanding of emerging threats. Businesses should see it as a gateway to swift government assistance, not a punitive measure.
- Emphasis on Collaboration: Promote a collaborative incident response model. Businesses should feel confident sharing information, knowing it bolsters collective defences without compromising their incident control measures.
- Government as Facilitator: Position the government as a coordinator in scenarios impacting numerous entities or individuals. Streamline communication channels between the affected parties, centralise information sharing, and provide guidance on addressing the collective impacts.

Balancing Enforcement with the Attacker's Threat:

- **Prioritizing Impactful Breaches:** Focus enforcement efforts on significant breaches or repeated non-compliance, specifically those with potential national security implications or large-scale consumer harm.
- **Leveraging Collective Insights:** Enforcement actions should be informed by the broader threat landscape revealed through reporting. Prioritise cases where attackers can be disrupted or where lessons learned can prevent similar attacks across multiple sectors.
- **Incentives for Early Engagement:** Encourage speedy, detailed reporting with offers of tailored government assistance, potential for reduced penalties (in specific circumstances), and access to shared threat intelligence resources.

Minimising Administrative Burden & Government as a Facilitator:

- **Centralised Incident Reporting:** Maintain a streamlined reporting process with a designated point of contact, minimising business redundancy. Integrate existing reporting requirements whenever feasible.
- **Leverage Information Sharing Platforms:** Use established secure platforms for incident reporting, streamlining communication and reducing the need to communicate separately with multiple agencies.
- **Active Facilitator Role:** In widespread incidents, the government should be a proactive facilitator, coordinating communication between affected businesses, technical experts, and even consumer protection authorities when necessary.

9. **What types of anonymised information about ransomware incidents would be most helpful for industry to receive? How frequently should reporting information be shared, and with whom?**

PEXA believes that by embracing automation, leveraging commercial and open-source platforms, and collaborating across the industry, the government can improve the speed and accessibility of ransomware threat intelligence across Australia.

Types of Valuable Anonymized Information:

- **Prioritizing Indicators of Compromise (IOCs):** Focus on readily actionable technical details, including file hashes, IP addresses, domain names, malware signatures, and specific network traffic patterns associated with ransomware campaigns. This allows swift integration into security monitoring and defence tools.
- **TTPs and Context:** Provide context around the IOCs. Include attack methods, targeted vulnerabilities, and any relevant attacker behaviour patterns. This aids in understanding the threat and proactively defending against similar activity.

- Additional Insights: Include anonymised details such as ransom demands, cryptocurrency wallets, industry sector trends, and geographical targeting information for broader threat awareness.

Leveraging Existing Platforms and Automation:

- Open-Source Collaboration: Emphasize sharing IOCs and threat context with well-established, widely used open-source platforms like MISP. This maximises visibility and rapid integration by a broad range of organisations.
- SIEM Integration: Design a structured, machine-readable threat feed (e.g., STIX/TAXII format) that SIEM platforms can quickly ingest. This streamlines threat analysis and automated response for many organisations.
- Beyond ACSC Email: While the ACSC's email alerts have value, prioritise modern, real-time sharing mechanisms built for speed and scale.
- Exploring Existing Platforms: Evaluate the effectiveness of the existing threat-sharing platform developed with Deloitte. Assess its suitability for broader dissemination, potential integration with open-source channels, and user feedback.

Additional Considerations:

- Data Quality and Timeliness: Prioritize verified, high-quality IOCs with minimal delay to maximise defensive value.
- Industry Partnerships: Collaborate with existing cyber security vendors to amplify the reach and utilisation of shared threat data.
- Clear Communication Channels: Ensure clear communication about how businesses can access and leverage the provided information.

Measure 3: Encouraging engagement during cyber incidents – Limited use obligation on the Australian Signals Directorate and the National Cyber Security Coordinator

10. What should be included in the ‘prescribed cyber security purposes’ for a limited use obligation on cyber incident information shared with ASD and the Cyber Coordinator?

    PEXA believes the approach should balance maximising cyber security benefits and maintaining trust. This should be achieved by primarily emphasising anonymous threat intelligence sharing while allowing for exceptions in the case of public safety.

    - Incident Response and Analysis: Enable ASD and the Cyber Coordinator to analyse attacks, provide immediate support, and offer tailored guidance to affected businesses.
    - Anonymised Threat Intelligence Sharing: Facilitate the sharing of anonymised information, particularly Indicators of Compromise (IOCs), to

enhance collective defence. This includes distribution across government, critical infrastructure operators, and relevant industry sectors.

- National Consequence Management: Use anonymised data to assess the broader impact of attacks and coordinate responses, especially those posing risks to essential services.
- Targeted Law Enforcement Collaboration: Allow sharing of specific, actionable details with relevant law enforcement agencies when investigating cybercrime, subject to established legal and privacy safeguards.

Possible Exception:

- Imminent Threat to Public Safety: Permit the sharing of necessary details, potentially including identifying information, when failure to act poses a significant, immediate risk to public health and safety.

Key Considerations:

- Emphasis on Anonymization: Prioritize anonymisation as the standard, ensuring businesses are protected and collaboration isn't hindered.
- Explicit Definition: Clearly define the limited use scope and review it regularly to address evolving threats.
- Clear Oversight: Institute transparent oversight mechanisms to ensure the obligation is upheld and data is responsibly used.

11. What restrictions, if any, should apply to the use or sharing of cyber incident information provided to ASD or the Cyber Coordinator?

PEXA believes the following restrictions should be considered. These factors will aid in providing a balance between enabling cyber security collaboration and protecting businesses that are reporting incidents. The Government should foster trust while ensuring appropriate privacy safeguards and continued pathways for law enforcement involvement when necessary.

- Prescribed Cyber security Purposes: Limit use strictly to incident response, threat intelligence sharing, consequence management, and (when legally permissible) support of law enforcement investigations.
- Anonymisation and Data Minimisation: Prioritize sharing anonymised information and collect only the minimum data necessary for cyber security goals.
- Protection from Regulatory Actions: Ensure reporting cannot be used against the impacted entity for fines, penalties, or non-compliance findings.
- Explicit Sharing Controls: Define permissible recipients of shared data (e.g., law enforcement with appropriate warrants, critical infrastructure partners) and subject them to equivalent use restrictions.

- Privacy and Security Safeguards: Implement robust technical and procedural safeguards to protect shared information from misuse, unauthorised access, or disclosure.
- Oversight and Transparency: Establish clear oversight mechanisms with regular audits and provide regular public reporting on using shared data to maintain trust.

12. What else can Government do to promote and incentivise entities to share information and collaborate with ASD and the Cyber Coordinator in the aftermath of a cyber incident?

PEXA believes that by emphasising timely support, consultative assistance, and respect for business autonomy, the government can foster trust and encourage information sharing without hindering recovery.

Focus on Support and Recovery:

- Tailored Assistance: Provide businesses that report incidents with direct access to technical expertise, threat intelligence, and recovery guidance. Help them restore operations quickly and minimise lasting damage.
- Validating Recovery Plans: Offer consultative support, helping businesses validate their incident response plans and make informed decisions, particularly for complex or large-scale events.
- Clear Communication Channels: Maintain streamlined contact points for businesses seeking assistance, avoiding bureaucratic hurdles during a crisis.

Prioritise Trust and Empowerment:

- Respect Business-Led Response: Position government resources as supplementary, not controlling. Businesses should retain autonomy over incident management.
- Industry Partnerships: Collaborate with ISACs and cyber security vendors, utilising their existing relationships and technical skills to support businesses on the ground.
- Lessons Learned: Share insights gleaned from reported incidents in a way that empowers self-improvement for the broader business community.

Additional Considerations:

- Education & Awareness: Promote the benefits of collaboration and government support as essential components of a strong cyber security posture.

Measure 4: Learning lessons after cyber incidents – A Cyber Incident Review Board

13. What should be the purpose and scope of the proposed Cyber Incident Review Board (CIRB)?

    The CIRB's primary goal should be to enhance cyber resilience for all Australians, boost national security, and reduce risks to the public by learning from past incidents and driving proactive improvements.

14. What limitations should be imposed on a CIRB to ensure that it does not interfere with law enforcement, national security, intelligence and regulatory activities?

    The CIRB should clearly focus on contributing to national cyber security resilience. This needs to be done without encroaching on the work of law enforcement, intelligence agencies, or regulators.

    - Focus on Closed Incidents: Restrict reviews to officially closed incidents with finalised investigations and no pending prosecutions.
    - Avoid Internal Operational Scrutiny: Explicitly exclude analyses of businesses' internal management, operations, or culture.
    - Prioritize Systemic Lessons: Emphasize extracting broader insights on vulnerabilities and attack patterns and actionable recommendations for improving cyber security across sectors.
    - Share Technical Insights: Disseminate anonymised IOCs (Indicators of Compromise) to help other entities bolster defences proactively and identify potential targeting.

    The CIRB should avoid taking the lead on communicating specific details to the media/public regarding active cyber incidents where possible. This should be left to the impacted organisations to manage, whilst the CIRB focusses on investigating and reviewing the matter.

15. How should a CIRB ensure that it adopts a ‘no-fault’ approach when reviewing cyber incidents?

    PEXA believes that by adhering to the following principles, the CIRB can add value to the public by learning from past incidents and driving proactive cyber security enhancements.

    - Emphasise Systemic Analysis: Focus reviews on technical vulnerabilities, attack patterns, and industry-wide gaps, avoiding scrutiny of individual actions or negligence.
    - Prioritise Recommendations: Propose proactive solutions and improvements for businesses and the broader cyber security community.

- Foster Collaboration: Engage with businesses as partners, seeking their input while protecting their confidentiality through anonymisation and aggregation.
- Maintain Independence: Ensure operational autonomy and separation from regulatory bodies to reinforce its non-punitive mission.
- Transparent Reporting: Publicly release anonymised findings and lessons learned to build trust and demonstrate a focus on collective improvement.

16. What factors would make a cyber incident worth reviewing by a CIRB?

The CIRB should aim to extract and share timely, actionable insights to minimise the impact of similar attacks and enhance the resilience of Australian businesses across various sectors.

- High Potential Impact: Incidents causing significant disruption to the economy, critical infrastructure, or public safety. These demand immediate analysis.
- Risk of Recurrence: Attacks targeting multiple sectors or likely to be widely replicated pose a widespread threat and warrant swift CIRB analysis.
- Novel Techniques or Threat Actors: Incidents employing new methodologies, zero-day exploits, or indicating unfamiliar threat actors offer crucial defensive insights.
- Actionable Lessons: Cases offering the potential to generate clear recommendations and timely threat intelligence to help businesses proactively improve defences or respond to emerging risks.

17. Who should be a member of a CIRB? How should these members be appointed?

PEXA believes that by including industry bodies and associations, the CIRB ensures a broad cross-section of representation, enhancing its understanding of sector-specific challenges and fostering broader buy-in for recommendations.

A CIRB should include members with expertise in:

- Cyber security: Technical experts with knowledge of attack methods, threat intelligence, and vulnerability analysis.
- Industry: Representatives from critical infrastructure sectors (e.g., healthcare, finance, energy) and key industry bodies for sector-specific insights and broader representation.
- Technology: Specialists understand software and hardware vulnerabilities.
- Legal & Regulatory: Experts in cyber security law and data protection.
- Government: Liaisons from relevant agencies (ASD, ACSC) to facilitate coordination while maintaining CIRB independence.

Appointment Considerations:

- Transparent Selection: Open, merit-based process to build trust.

- **Independence & Integrity:** Choose members with solid reputations and no conflicts of interest.
- **Diverse Backgrounds:** Include varied perspectives for well-rounded analysis.
- **Term Limits:** Implement rotation to ensure fresh insights.
- **Balance of Expertise and Efficiency:** Aim for a board size that enables thorough reviews while facilitating the timely release of actionable intelligence.

18. **What level of proven independent expertise should CIRB members bring to reviews?**
    Please refer to the responses to question 17.

19. **How should the Government manage issues of personnel security and conflicts of interest?**
    The government must ensure the CIRB's impartiality and maintain public trust in its mission to enhance national cyber resilience.

    To manage personnel security and COIs on the CIRB, the government should:
    - **Robust Vetting:** Implement thorough background checks and security clearances as needed, like the process used for non-profit boards.
    - **Conflict of Interest Management:**
        - Clear Definition in Charter: The CIRB's charter must explicitly outline potential conflicts of interest, including financial gain from outcomes.
        - Transparent Disclosure & Recusal: Mandate disclosure of any potential conflicts, with clear recusal procedures to ensure objectivity.
        - Vendor Restrictions: Carefully consider membership of cyber security vendors to avoid bias and the appearance of profiteering from CIRB findings.
    - **Ongoing Monitoring:** Proactive monitoring of COIs, with independent oversight mechanisms for review and dispute resolution.

20. **Who should chair a CIRB?**
    Ideally, there should be a selection of chairs that can rotate in and out over time and selection of the chair should be based on skills as opposed to specific appointments. It would be reasonable for the CIRB to meet and elect a chair for a specific term with specific KPIs and defined expectations. The chair, along with the other members, should be able to guide and provide enough insight and information on the appropriate output for incidents being reviewed.

21. **Who should be responsible for initiating reviews to be undertaken by a CIRB?**

A hybrid approach with a rotating CIRB committee, in collaboration with government agencies, offers a robust model for initiating CIRB reviews.

- CIRB-led proactivity: A rotating committee within the CIRB empowers it to proactively identify incidents with high learning potential based on emerging threat patterns and industry needs.
- Government collaboration: Close collaboration with ASD, ACSC, and Home Affairs ensures alignment with national security priorities and access to broader incident data.
- Balanced Decision-Making: This hybrid model combines the CIRB's in-depth technical expertise with the government's broader threat awareness, creating a well-informed selection process.
- Adaptability: A regularly rotating committee allows diverse perspectives and reduces the risk of stagnation in case selection.

Considerations for Implementation:

- Clear Criteria: Establish transparent guidelines for incident selection, emphasising factors like national security impact, systemic vulnerabilities, and potential for actionable recommendations.
- Reporting and Feedback: Implement a process for the committee to report on selection decisions and rationale to the full CIRB and relevant government stakeholders, ensuring accountability.
- Public Input: Consider a limited mechanism for the public or cyber security community to suggest potential reviews, subject to vetting, to capture emerging trends.

22. What powers should a CIRB be given to effectively perform its functions?

To perform its functions effectively, the CIRB should have the following powers:

- Access to Anonymised Data: Unrestricted access to anonymised incident reports and technical information, including Indicators of Compromise (IOCs).
- Limited Subpoena Power: In rare cases, with strict legal oversight, the ability to compel specific information or engage individuals from organisations directly impacted by major incidents. Particularly when matters of public safety are involved.
- Focus on retrospective analysis: Emphasise the CIRB's role in learning from past incidents, not actively interfering in ongoing law enforcement or regulatory proceedings.
- Impartiality and Independence: Maintain operational autonomy to ensure objective analysis and build trust.

Additional Considerations:

- **Mandate for Critical Infrastructure:** Consider mandated collaboration between the CIRB and critical infrastructure operators for incidents with widespread potential impact.
- **Voluntary Participation for Others:** Allow optional CIRB review for non-critical sectors, encouraging broad participation while respecting business sensitivities.

23. **To what extent should the CIRB be covered by a 'limited use obligation', similar to that proposed for ASD and the Cyber Coordinator?**

Encouraging voluntary participation in CIRB reviews is crucial, particularly from sectors where collaboration isn't mandated. This approach will significantly enhance the CIRB's ability to gain a broad, systemic understanding of the threat landscape.

A 'limited use obligation' is essential for the CIRB to:

- **Protect Businesses and Individuals:** Guarantee that sensitive information shared during reviews cannot be used for regulatory action, fines, or legal proceedings against those impacted by cybercrime.
- **Build Trust:** Create a safe space for businesses to share incident details without fear of repercussions, fostering open collaboration and maximising learning opportunities.
- **Prioritise Anonymisation:** It should be mandated that the CIRB's reports that are made public, protect the identity of the impacted organisations (e.g. anonymise / de-identify data). This includes removing details that may place the organisation who experienced the incident at further risk. The only exception to this, would be agreement by the impacted organisations to be identified for the sake of helping other Australian organisations.

24. **What enforcement mechanism(s) should apply for failure to comply with the information gathering powers of the CIRB?**

A hybrid approach will help balance vigorous enforcement where participation is mandated. At the same time, offering a clear framework for voluntary participation encourages collaboration without overly harsh penalties.

Enforcement Mechanisms:

- **Mandatory Cooperation (SOCI Act):** For critical infrastructure subject to SOCI Act obligations, non-compliance with CIRB information requests should mirror existing enforcement mechanisms under the Act.
- **Voluntary Participation:** Consider a voluntary deed system like the ACSC partnership model for non-critical sectors. This deed would:
  - Outline benefits of CIRB collaboration (early access to insights, tailored guidance, etc.)
  - Standardise information-sharing expectations.

  - Stipulate consequences for non-compliance, potentially including revocation of CIRB membership benefits.

Additional Considerations:

- **Proportionate Enforcement:** Scale actions based on incident severity and whether non-compliance appears deliberate.
- **Good Faith Efforts:** Recognize good faith attempts at compliance, helping before resorting to strict enforcement.

25. **What design features are required to ensure that a CIRB remains impartial and maintains credibility when conducting reviews of cyber incidents?**
    Refer to previous answers in this section on the design, implementation, and governance of the CIRB.

26. **What design features are required to ensure a CIRB can maintain the integrity of and protection over sensitive information?**
    PEXA advises to implement these technical and procedural measures. The CIRB can then demonstrate a commitment to data protection, essential for building trust and encouraging collaboration.

Technical Safeguards:

- **Strict Access Controls:** Implement role-based access controls and the principle of least privilege to limit data access based on need-to-know.
- **Secure Storage:** Utilize encrypted storage solutions for sensitive data at rest and in transit.
- **Audit Trails:** Maintain robust audit logs to track all data access and modifications.

Procedural Safeguards:

- **Clear Data Handling Protocols:** Establish detailed protocols for data collection, storage, analysis, and sharing.
- **Anonymisation and Aggregation:** Mandate anonymisation and data aggregation, removing identifiable details whenever possible.
- **Non-Disclosure Agreements (NDAs):** Require all CIRB members and personnel to sign strict NDAs.

Additional Considerations:

- **Regular Security Assessments:** Conduct regular vulnerability assessments and security audits.
- **Incident Response Plan:** Have a clear incident response plan for potential data breaches.
- **Personnel Training:** Provide mandatory security awareness training to all CIRB staff.

Response to measures: Part 2 – Amendments to the SOCI Act

Measure 5: Protecting critical infrastructure – Data storage systems and business critical data

27. How are you currently managing risks to your corporate networks and systems holding business critical data?

    PEXA currently uses a layered controlled environment to protect critical data. This includes a combination of network and access controls. For example, segregation, privilege access management (PAM) tools, Data Loss Prevention (DLP) monitoring and asset management. The key is to ensure that all critical data stores are known, classified, catalogued, and have appropriate controls to ensure they are only accessed and modified by authorised parties. In addition to this, PEXA also ensures that quarterly access reviews are conducted to ensure principles of least privilege are upheld.

28. How can the proposed amendments to the SOCI Act address the risk to data storage systems held by critical infrastructure while balancing regulatory burden?

    PEXA believes that the suggested reforms to cover secondary systems will help increase resilience to critical infrastructure. This is because threat actors are likely to look for weaker systems to compromise as a pivot point into broader IT environments. Ensuring that secondary systems are covered will further decrease the likelihood of this happening. This should potentially extend to non-production as they can be used as an attack vector. Especially if organisations are using production data in non-production systems. Even though this is not considered best practice, it is happening more frequently in some businesses.

    However, the measures to provide this protection should be clear and not overlap with any existing regulatory requirements. Any amendments in this space should be done in consultation with regulators to reduce the likelihood of duplication. The reason for this is that double up can reduce the amount of time organisations have to perform proactive security work and subsequently increasing risk.

29. What would be the financial and non-financial impacts of the proposed amendments? To what extent would the proposed obligations impact the ability to effectively use data for business purposes?

    PEXA believes that this would depend on the size of the business and the number of systems that need to be protected. Therefore, it would be necessary for the SOCI Act to be clear on what constitutes a secondary system. This could mean identifying any primary and secondary stores (such as backups) of critical data. However, if the guidance from the government is too broad, it is likely to result in significant rework of controls which could lead to unnecessary financial impact. Ultimately, there needs to be a balance to ensure that all investments have a measurable impact on system resilience.

Measure 8: Enforcing critical infrastructure risk management obligations - Review and remedy powers

30. How would the proposed review and remedy power impact your approach to preventative risk?

Any review and remedy powers should consider an organisations existing risk management practice, the risk profile of the business and any existing accreditations or audit results it has achieved over the past 2 years, particularly if obtained through an external and independent provider (for example, fit for purpose risk management assessments of it overall Risk Management Framework or ISO 31000 standard).

'Seriously deficient' elements of a organisations risk management approach should be clear and unequivocal to support an organisation understand the full risk requirements of an organisation subject to critical infrastructure obligations.