CYAINSE SECURING AI SAFEGUARDING FUTURE

Feedback in response **to** Cyber Security Legislative Reforms: consultation on proposed new cyber security legislation and on changes to the Security of Critical Infrastructure Act 2018.

Part 1: New cyber security Legislation

Measure 1 – Secure by design standards for IoT devices

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

Response:
Although supply chain's security is a shared responsibility among manufacturers, suppliers, developers, distributors, regulatory bodies, and end users, by giving manufacturers the lion's share of the blame, security is given top priority during the design and production phases. By using contracts and agreements, manufacturers may ensure that software developers and subcontractors are held accountable, so ensuring that security is taken care of at every stage. Manufacturers need to build smart devices which can detect and resist tampering.

- 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?

Response:
The definition should be tailored to the Australian context, informed by stakeholder consultation, aligned with existing legal and regulatory frameworks, and based on a risk-based approach. Given the quick speed at which technology such as AI is developing and evolving, the definition needs to be sufficiently adaptable and future-proof to take new kinds of smart devices and developing technologies into account. Industry standards such as NIST can be referenced for a broader definition.

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

Response:
Low-risk and low value devices with minimal internet connectivity, data collection, or security-sensitive functions such as light bulbs, smart plugs etc, devices with short lifespans such as temporary event trackers, promotional devices and devices which are already

regulated in industries such as medicine and aviation maybe exempted from proposed cyber security standard.

Measure 2 – Ransomware reporting for businesses.

- What mandatory information should be reported if an entity has been subject to a ransomware or cyber extortion incident?

Response:
In addition to incident summary with overview of incident and how it was discovered following additional details must be provided.

1. Basic details: Date and time stamp of incident, type and severity of incident, affected assets and data, impact, number of users or customers affected, ransomware demand details (amount of ransom asked), Payment mode and details eg. Crypto payments if payment made against demand of ransom.
2. Technical details (if available): Indicators of compromise, APT group attribution details, domains, URLs etc.
3. Breach or risk management: Impact analysis on scope and severity of impact, what and how much data records compromised.
4. Response details: Notification timeline details to customers, partners, regulators. Recovery actions taken in response.
5. Lessons learned: root cause analysis, lesson learned, details on gaps identified, measures to prevent the ransomware.

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

Response:
Following additional information should be reported:
(a) Payment currency (eg. AUD, Bitcoin)
(b) Payment method (eg. Cryptocurrency exchange, money transfer service)
(c) Transaction details: Include any relevant transaction identifiers or wallet addresses involved in the payment.
(d) Amount of money or equivalent paid
(e) Communication details: Communication channel ((e.g., email, dark web chat).

- Which entities should be subject to the mandatory ransomware reporting obligation?

Response:
Following entities should be subject to this reporting obligation:
(a) Crtitcal infrastructure sectors or organizations covered under SOCI Act (eg. Banks)
(b) Healthcare providers
(c) Managed services providers
(d) Educational institutions
(e) Organizations storing or processing customer or sensitive information.
(f) 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 payment?

Response:
48-72 hours is a reasonable timeframe to report ransomware attack or after paying ransom. This time allows initial investigation time and ensures prompt reporting post investigation.

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

Response:

(a) Administrative fines: Graduated fines based on the severity of the non-compliance and the size of the organization can incentivize timely reporting.
(b) Public disclosure: Publishing the names of non-compliant entities can encourage adherence and deter future violations.
(c) **Exclusion from** government contracts**:** Restricting access to certain government contracts or benefits for non-compliant entities can create a significant incentive for compliance.
(d) Reduced Tax rebates or tax benefits.

- What types of anonymised information about ransomware incidents would be most helpful for industry to receive? How frequently should reporting information be shared, with whom, and in what format

Response:
Types of anonymized information helpful to industry:

(a) Attack techniques: General descriptions of the methods used by attackers (e.g., phishing campaigns, malware types, vulnerabilities exploited) without disclosing specific details.
(b) Targeted sectors: The industries or types of organizations most frequently targeted, without identifying individual companies.
(c) Impact of attacks: General categories of impacts, such as data breaches, operational disruptions, or financial losses, without disclosing specific details.
(d) Ransomware strains: The types of ransomware involved, categorized by families or variants, without disclosing technical specifics.
(e) Recovery strategies: High-level insights into successful mitigation and recovery approaches, anonymized to protect sensitive information.

Frequency and format of information sharing:

(a) Regular reporting: Sharing anonymized data periodically, such as quarterly or biannually, can provide valuable insights without overwhelming recipients.
(b) Variety of formats: Consider offering reports, infographics, or interactive dashboards to cater to different user preferences and information needs.

Measure 3 – Limited use obligation on ASD & NCSC

- 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?

Response:

(a) Identifying & analyzing threats: Understanding attacker tactics and developing threat intelligence.
(b) Responding to and mitigating incidents: Providing support to affected entities and improving overall response strategies.
(c) Regulatory compliance & enforcement: Investigating cybercrime and enforcing relevant laws (with proper authorization).
(d) Cybersecurity research & development: Informing the development of new tools and national cybersecurity strategies.
(e) Public awareness & education: Educating the public about cyber threats and promoting safe online practices.

- What restrictions, if any, should apply to the sharing of cyber incident information?

Response:

(a) Limited use: Information can only be used for specific cybersecurity purposes, not for commercial gain or to penalize the reporting entity.
(b) Minimize data shared: Only share the essential details, potentially anonymizing or aggregating data to protect sensitive information.
(c) Strict access controls: Only authorized personnel can access the information, with robust security measures in place.

- 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?

Response:
Acknowledge and publicly recognize entities that demonstrate exemplary cybersecurity practices and responsible information sharing. Establish awards or other recognition programs to incentivize entities to proactively share information and collaborate with government agencies.

Part 2: Amendments to the Security of Critical Infrastructure Act 2018

Measure 5: Data storage systems and business critical data

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

Response:
Following are some steps being taken to manage risks:

(a) Implementing security controls: This includes measures such as firewalls, intrusion detection and prevention systems, and data encryption to protect systems and data from unauthorized access, use, disclosure, disruption, modification, or destruction.
(b) Regularly patching systems: Keeping systems up to date with the latest security patches is essential to address known vulnerabilities that attackers can exploit.
(c) Educating employees about cybersecurity: Employees should be aware of the security risks and how to protect themselves and the organization from cyberattacks.
(d) Having a security incident response plan: This plan outlines the steps that should be taken in the event of a security incident, such as a data breach or ransomware attack.
(e) Regularly backing up data: Having a backup of your data allows you to recover it in the event of a security incident or system failure.
(f) Using a risk assessment framework: This framework can help you identify, assess, and prioritize the risks to your organization's systems and data.

Measure 6: Consequence management powers

- How would a directions power assist you in taking action to address the consequences of an incident?

Response:
It empowers stakeholders to act decisively, efficiently, and legally in addressing incident consequences.
(a) Clarifying Authority: Defines who can issue directives.
(b) Enabling Coordination: Facilitates collaboration among stakeholders.
(c) Providing Legal Backing: Grants legal authority for actions taken.
(d) Expediting Decision-Making: Speeds up response efforts.
(e) Enforcing Compliance: Ensures parties follow directives.
(f) Supporting Resource Allocation: Authorizes deployment of necessary resources.
(g) Enhancing Accountability: Makes roles and responsibilities clear.
(h) Promoting Resilience Building: Encourages preparation for future incidents.

- What other legislation or policy frameworks (e.g., at a state and territory level) would interact with the proposed consequence management power and should be considered prior to its use?

Response:
Federal:
(a) Cybersecurity Act 2018: Aligning with incident reporting, information sharing, and risk management provisions.
(b) Telecommunications Act 1997: Considering data breach and user privacy provisions.

(c)Privacy Act 1988: Respecting data privacy principles.
State/Territory:
(a) Privacy laws: Complying with individual legislative frameworks for handling personal information.
(b) Critical infrastructure legislation: Complementing existing security measures.
(c) Emergency management legislation: Coordinating with relevant authorities if needed.
Policy Frameworks:
(a) Australia's Cyber Security Strategy 2020: Aligning with national cybersecurity objectives.
(b) State/Territory cybersecurity strategies: Considering additional context and guidance.

- What principles, safeguards and oversight mechanisms should Government establish to manage the use of a consequence management power?

Response:
(a) Principles: Necessity, proportionality, transparency, accountability, due process, respect for rights.
(b) Safeguards: Clear definitions, independent oversight, impact assessments, cybersecurity hygiene incentives.
(c) Oversight mechanisms: Parliamentary, judicial, public reporting (balancing transparency with security)

Measure 7: Protected information provisions

- How can the current information sharing regime under the SOCI Act be improved?

Response:
(a) Make it easier to share: Simplify reporting, offer clear guidance, and address legal concerns.
(b) Build trust and collaboration: Engage with stakeholders, be transparent, and facilitate joint exercises.
(c) Incentivize participation: Offer financial rewards, promote good practices through insurance, and recognize responsible entities publicly.
(d) Improve sharing mechanisms: Invest in secure platforms, explore anonymized data sharing, and encourage cross-sector collaboration.
(e) Adapt to the evolving landscape: Regularly review regulations, harmonize with international efforts, and stay ahead of emerging threats.

Thanks
Rakesh
CYAINSE
contact@cyainse.com