Submission to 2023-2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper

Macquarie University Cyber Security Hub
ThreatDefence Pty Ltd

Introduction

The Macquarie University Cyber Security Hub promotes a unique interdisciplinary approach in cyber security and forms an ideal ecosystem for its partners in business, government, research and education to collaborate effectively towards a resilient, secure and trustworthy cyber infrastructure.

Our submission is in collaboration with our industry ally, ThreatDefence, a leading Australian provider of cyber security solutions and cyber range training services.

Our Submission

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

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

The proposed Cyber Incident Review Board (CIRB) should aim to enhance cybersecurity education for defenders, including practitioners actively engaged in safeguarding against cyber threats.

The CIRB's responsibilities would include evaluating initial anonymized reports or exercising discretion to identify incidents that warrant further investigation, especially those that introduce new attacking methods or techniques by threat actors. The emphasis should be on investigating incidents that set precedents in cybersecurity threats, thereby offering valuable lessons and insights.

A critical function of the CIRB would be to disseminate analysis data to the wider industry to bolster cybersecurity education and ensure the community remains informed about the latest developments and threats. This could involve providing training organizations and universities with detailed descriptions of attack methods. Such information could be utilized in cyber security training simulations (cyber ranges), preparing defenders to effectively respond to similar attacks in the future. This approach not only aids in the direct education of current and future cybersecurity professionals but also fosters a proactive and informed cybersecurity community capable of adapting to evolving threats.

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

Cyber Incident Review Board (CIRB) can ensure it adopts a 'no-fault' approach to reviewing cyber incidents by emphasizing industry engagement, education, and the training and simulation of cybersecurity attacks. This strategy should prioritize learning and improvement over assigning blame. By concentrating on disseminating knowledge, sharing best practices, and facilitating simulations of cyber-attack scenarios, the CIRB can foster a culture of continuous learning and resilience within the cybersecurity community. This approach encourages organizations to openly share their experiences without fear of repercussion, leading to a more informed and prepared industry capable of collectively addressing cybersecurity challenges.

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

A cyber incident would warrant review by a Cyber Incident Review Board (CIRB) based on several key factors:

- **Novelty: Incidents involving unprecedented or innovative cyber threats that could provide new insights into attacker methodologies or emerging trends.**
- **New Attack Methods: Incidents that showcase previously unknown or significantly evolved attack vectors, techniques, tactics, and procedures (TTPs) that add to the collective understanding of cyber threats.**
- **Community Value: Incidents whose analysis and lessons learned could greatly benefit the wider cybersecurity community by enhancing preparedness and response strategies.**
- **Educational Potential: Incidents that offer valuable case studies for cybersecurity education and training, including the development of simulations and training exercises to better equip defenders against similar threats.**

These factors collectively ensure that the CIRB focuses on incidents that not only enrich the cybersecurity knowledge base but also contribute to the strengthening of defenses across the community.

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

Members of a Cyber Incident Review Board (CIRB) should be carefully selected to include individuals from academia and organizations specializing in cybersecurity training. This composition ensures the board benefits from a strong focus on education and understands the necessities for effectively training cyber defenders.

To appoint these members, a structured nomination process should be implemented. This process could involve:

- **Open Nominations: Allowing relevant organizations and educational institutions to nominate candidates who have demonstrated expertise and commitment to cybersecurity education and defense training.**

- **Peer Review: Candidates' qualifications and contributions to the cybersecurity field should be assessed by a committee of their peers, ensuring that selected members have the respect and recognition of the cybersecurity community.**
- **Diverse Representation: Effort should be made to ensure the board includes a diverse range of expertise, encompassing different areas of cybersecurity, to provide a holistic approach to incident review and educational content development.**

Such a selection process would not only ensure the CIRB is composed of members with the requisite knowledge and experience but also foster a culture of inclusivity and collaboration within the cybersecurity education and training community.

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

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

We recommend that a significant focus of such reporting should be on learning the technical details of incidents that can be quickly packaged into actionable intelligence and distributed to the public in an anonymized manner.

One critical observation we have made from our incident response experience is that even when this information is reported to ACSC, it is usually distributed to the ACSC partner network without much context, primarily in the form of technical indicators rather than more generic signals about adversary behavior.

In practice, such reporting often occurs significantly after the incident, with much information becoming obsolete or less valuable.

To facilitate this reporting, it should be available in an anonymized manner, allowing incident responders to share their insights easily and quickly.

Another important aspect is that the bulk of cybersecurity incidents occur due to the exploitation of standard weaknesses, often new vulnerabilities that often become known to the public through multiple channels (vendor security advisories, news, etc.). Knowing about the use of these vulnerabilities and exploits in Australia might be useful, but not so much for security practitioners.

What is much more important and valuable is information on any novel methods and techniques employed by threat actors.

Another aspect is bypassing existing security tools. Many security tools are being bypassed by threat actors, and it is always useful to understand which controls were not effective.

We also notice increasingly that ransomware operators tend to spend less time in their victim networks, trying to quickly exfiltrate some data and then act on their objectives (ransomware deployment). This contrasts with what we dominantly saw in previous years when they would spend significantly more time in their victim's environments. It would be very useful to know about the extent of any particular incident.

Thus, mandatory reporting information should be decided based on what defines the incident, as follows:

Anonymized Real-Time Reporting - as soon as possible, during the investigation:

- **Threat actor identification (if possible)**
- **Any immediate intelligence indicators available to the responder.**

Non-anonymized Post-Investigation Reporting:

- **Threat actor identification (if possible)**
- **Threat categorization - whether a well-known vulnerability or method of attack was used, or something novel was employed**
- **The extent of the attack (in terms of how many systems were compromised, and what data was accessed by the threat actor)**
- **Which security tools were blocked or bypassed by the threat actor.**

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

We also want to emphasize that this information needs to be reported in an anonymized manner. In cases where a ransom was paid, it is beneficial for other incident responders to understand how the ransom was negotiated, the amount paid, and, specifically, what measures the victim took to communicate with the threat actor regarding the deletion of the extorted data.

11. 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?

We advocate for the availability of voluntary, anonymized reporting for all cybersecurity responders. This approach supports the community of practitioners by fostering a collaborative environment and encouraging the sharing of insights among peers.

All larger organizations, whose cybersecurity faults can negatively impact the wider public, should be subject to mandatory post-incident reporting.

12. 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?

We hold the view that reporting mechanisms should motivate businesses to share their findings promptly, facilitated by continuous engagement with cyber practitioners and community support.

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

We believe these principles are crucial to guarantee that reporting occurs effectively and fulfills its intended purpose. Coupled with the principle of anonymized reporting for real-time threat intelligence, these guidelines should facilitate sustained engagement within the industry and among incident responders.

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

We suggest achieving this balance by enabling the Cyber Incident Review Board (as defined in Measure 4) to utilize non-anonymized data and conduct further inquiries into the incidents.

16. 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?

As per our response to #8 above. The Government needs to ensure that the cyber security community members have prompt access to this intelligence and the appropriate anonymised context.