Federation University and ThreatDefence

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

Foreword

Federation University welcomes the opportunity to provide input **on** the question raised in the consultation paper. Federation University is committed to cyber security education in our regional communities, as well as to cyber security research, including topics that address some of the most significant challenges facing Australia and the world.

We are submitting this response jointly with our industry partner, ThreatDefence, an Australian cyber security vendor and service provider of cyber range training products.

Our Submission

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 would like to present our formal recommendations in response to the point 8 as follows:
We strongly advocate for a significant emphasis on gathering technical details of such incidents, which can subsequently be transformed into actionable intelligence. This intelligence should then be disseminated to the public in an anonymized format. Through our extensive incident response experience, we have observed a notable gap in contextualizing reported information. Often, data provided to the Australian Cyber Security Centre (ACSC) and its partner network lacks comprehensive context, predominantly manifesting as technical indicators rather than encompassing broader insights into adversary behavior.

Furthermore, we have noticed that reporting frequently transpires after the incident, rendering much of the information obsolete or less valuable. To streamline this process, reporting mechanisms should facilitate anonymized submissions, enabling incident responders to share their insights swiftly and effortlessly.

In addition to technical indicators, it is imperative to focus on identifying any novel methods and techniques employed by threat actors. While awareness of vulnerabilities is important, the emphasis should be placed on understanding the tactics utilized by adversaries, particularly in bypassing existing security measures.

Moreover, the evolving modus operandi of ransomware operators, characterized by expedited exfiltration of data followed by ransomware deployment, underscores the necessity of comprehensive reporting. Therefore, we propose a delineation of mandatory reporting information based on the following criteria:

Anonymized Real-Time Reporting (During Investigation):

- Identification of threat actors, if ascertainable.
- Immediate intelligence indicators available to the responder.

Non-Anonymized Post-Investigation Reporting:

1. Identification of threat actors, if possible.
2. Categorization of threats, distinguishing between well-known vulnerabilities or methods of attack and novel techniques.
3. Assessment of the attack's extent, including the number of compromised systems and the nature of data accessed by threat actors.
4. Identification of security tools that were circumvented or rendered ineffective by threat actors.

We believe that adopting these reporting measures will enhance the efficacy of incident response efforts and contribute significantly to fortifying cybersecurity resilience in Australia.

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

It is paramount that such information is reported in an anonymized manner to ensure confidentiality and privacy for all parties involved. Transparency in reporting is crucial for facilitating collective learning and enhancing incident response capabilities.

Specifically, in instances where a ransom payment is made, it is imperative to provide insight into the negotiation process, including details on how the ransom was negotiated, the amount paid, and the measures undertaken by the victim to communicate with the threat actor regarding the deletion of the extorted data. Such information is invaluable for incident responders in understanding the dynamics of ransomware attacks and devising effective mitigation strategies.

By anonymizing the reporting process, organizations can contribute to a comprehensive knowledge base without compromising sensitive information. This collaborative approach fosters a more resilient cybersecurity ecosystem, enabling stakeholders to proactively address emerging threats and protect against future incidents.

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 establishment of a framework that facilitates voluntary, anonymized reporting for all cybersecurity responders. Such an approach is instrumental in fostering a collaborative

environment within the cybersecurity community, thereby promoting the exchange of valuable insights and best practices among peers. By encouraging voluntary reporting, organizations of all sizes can contribute to a collective knowledge base, ultimately enhancing the overall resilience of the cybersecurity landscape.

However, it is our firm belief that mandatory post-incident reporting should be enforced for larger organizations, particularly those with an annual turnover exceeding $10 million. Given their significant impact on the wider public and the potential ramifications of cybersecurity faults, it is imperative that these entities are held accountable for transparently reporting ransomware incidents. Mandatory reporting requirements ensure greater transparency and accountability, enabling relevant stakeholders to assess the scope and severity of cyber threats effectively.

In conclusion, while voluntary, anonymized reporting should be made available to all cybersecurity responders to facilitate knowledge-sharing and collaboration, larger organizations with substantial public-facing operations must be obligated to adhere to mandatory reporting standards to uphold accountability and transparency in cybersecurity practices.

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 firmly advocate for reporting mechanisms that incentivize businesses to share their findings promptly following such incidents. Timely reporting is essential for facilitating swift and effective response efforts, minimizing the potential impact of cyber threats, and safeguarding against future attacks. Moreover, continuous engagement with cyber practitioners and community support plays a pivotal role in encouraging timely reporting practices.

While it is crucial to establish a specific timeframe for reporting, it should be balanced to accommodate the complexities associated with incident response activities. A reasonable time period should be delineated, taking into account the need for thorough investigation and analysis to ensure the accuracy and comprehensiveness of the reported information. Additionally, clear guidelines and support mechanisms should be provided to assist organizations in meeting reporting obligations within the stipulated timeframe.

Furthermore, fostering a culture of transparency and collaboration within the cybersecurity community can further facilitate timely reporting by empowering organizations to share their experiences and insights openly. By leveraging collective knowledge and expertise, stakeholders can work together to address emerging threats and enhance overall cybersecurity resilience.

In conclusion, we believe that reporting mechanisms should be designed to encourage prompt sharing of findings, supported by ongoing engagement with cyber practitioners and community support networks.

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 firmly believe that the adoption of no-fault and no-liability principles is paramount to ensuring effective reporting practices and achieving the intended objectives of such initiatives. These principles provide a critical assurance to reporting entities, alleviating concerns regarding potential repercussions or liabilities associated with disclosing cybersecurity incidents. By establishing a supportive and non-punitive reporting environment, organizations are more likely to come forward and share relevant information, thereby facilitating a comprehensive understanding of emerging cyber threats and enhancing collective resilience.

Furthermore, when coupled with the principle of anonymized reporting for real-time threat intelligence, these guidelines serve to bolster confidence levels among incident responders and industry stakeholders. Anonymized reporting not only safeguards sensitive information but also encourages open and transparent communication within the cybersecurity community. By anonymizing reported data, organizations can contribute valuable insights without fear of adverse consequences, fostering sustained engagement and collaboration in combating cyber threats.

In conclusion, the incorporation of no-fault and no-liability principles in ransomware reporting frameworks is instrumental in promoting a culture of trust, transparency, and collaboration within the cybersecurity ecosystem. These principles, when complemented by anonymized reporting practices, are pivotal in fostering sustained engagement and facilitating the exchange of actionable threat intelligence among industry stakeholders and 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 propose that achieving this delicate balance necessitates empowering the Cyber Incident Review Board (CIRB), as defined in Measure 4, with the authority to utilize non-anonymized data and conduct thorough inquiries into reported incidents. By leveraging non-anonymized data, the CIRB can perform comprehensive assessments of cybersecurity incidents, thereby facilitating a more nuanced understanding of the underlying causes and contributing factors.

While the implementation of no-fault and no-liability principles is crucial for fostering a conducive reporting environment and encouraging transparency, it is equally important to uphold public expectations regarding business accountability in cybersecurity. The CIRB, equipped with access to non-anonymized data, can play a pivotal role in achieving this balance by holding organizations accountable for their cybersecurity practices while also providing necessary support and guidance to enhance resilience and mitigate future risks.

Furthermore, the CIRB can serve as a mechanism for promoting best practices and driving continuous improvement in cybersecurity standards across various sectors. Through its inquiries and recommendations, the Board can help businesses identify areas for improvement and

implement proactive measures to strengthen their cybersecurity posture, thereby aligning with public expectations for accountability and responsibility.

In conclusion, enabling the CIRB to utilize non-anonymized data and conduct thorough inquiries into reported incidents is instrumental in striking a balance between no-fault and no-liability principles and public expectations for business accountability in cybersecurity. By leveraging this approach, the government can foster a collaborative environment that encourages responsible cybersecurity practices while also providing the necessary support and guidance to enhance resilience and protect against cyber threats.

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 articulated in our response to point #8, it is imperative that the government ensures timely access to actionable intelligence and appropriate anonymized context for members of the cybersecurity community. Anonymized information serves as a valuable resource for industry stakeholders, enabling them to enhance their understanding of emerging cyber threats and adopt proactive measures to mitigate risks effectively.

The types of anonymized information that would be most beneficial for industry include insights into the tactics, techniques, and procedures employed by threat actors, as well as indicators of compromise and patterns of malicious activity. Additionally, contextual information regarding the impact and severity of ransomware incidents, along with recommended mitigation strategies, can empower organizations to bolster their cybersecurity defenses and respond more effectively to evolving threats.

In terms of frequency, reporting information should be shared promptly following the occurrence of ransomware incidents, with updates provided as new insights and intelligence become available. Timely dissemination of information is essential for enabling proactive threat detection and response, minimizing the potential impact of cyber-attacks, and safeguarding critical infrastructure and data assets.

As for the recipients of reporting information, it might be disseminated to relevant stakeholders within the cybersecurity community, including government agencies, industry associations, and private sector organizations. By fostering collaboration and information sharing among these entities, the government can facilitate a coordinated response to ransomware threats and enhance collective resilience against cyber-attacks.

In conclusion, the government must ensure that members of the cybersecurity community have prompt access to anonymized intelligence and contextual information about ransomware incidents. By facilitating timely information sharing and collaboration, the government can

empower industry stakeholders to effectively mitigate risks and protect against emerging cyber threats.

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 primary objective of the proposed CIRB should be to enhance cybersecurity education for defenders, particularly practitioners actively involved in safeguarding against cyber threats. To achieve this goal, the CIRB's responsibilities would encompass evaluating initial anonymized reports or exercising discretion to identify incidents that merit further investigation, particularly those that introduce novel attacking methods or techniques by threat actors. By focusing on incidents that set precedents in cybersecurity threats, the CIRB can provide valuable lessons and insights to the broader cybersecurity community.

A critical function of the CIRB would be to disseminate analysis data to the wider industry, thereby bolstering cybersecurity education and ensuring that the community remains informed about the latest developments and threats. This dissemination effort could involve providing detailed descriptions of attack methods to training organizations and universities, which can then be utilized in cyber security training simulations (cyber ranges). By incorporating real-world scenarios into training programs, defenders can gain practical experience and develop the skills necessary to effectively respond to similar attacks in the future.

Furthermore, 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. By promoting continuous learning and knowledge-sharing, the CIRB plays a vital role in strengthening the overall resilience of the cybersecurity ecosystem.

In conclusion, the proposed Cyber Incident Review Board should focus on enhancing cybersecurity education for defenders, evaluating incidents that introduce new attacking methods, and disseminating analysis data to the wider industry to foster a proactive and informed cybersecurity community capable of effectively responding to evolving threats.

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

The CIRB can ensure it adopts a 'no-fault' approach by prioritizing industry engagement, education, and the training and simulation of cybersecurity attacks. This strategy places a premium on learning and improvement rather than assigning blame, thereby fostering a culture of transparency and collaboration within the cybersecurity community.

Emphasizing knowledge dissemination and sharing best practices, the CIRB can facilitate simulations of cyber-attack scenarios, allowing organizations to gain practical experience in responding to various threats. By providing a platform for hands-on learning and skill development, the CIRB 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.
Furthermore, by focusing on continuous learning and resilience-building initiatives, the CIRB can help organizations develop robust incident response capabilities and enhance their overall cybersecurity posture. Through collaborative efforts and knowledge-sharing initiatives, the cybersecurity community can effectively mitigate risks and adapt to evolving threats in a proactive manner.
In a nutshell, the CIRB can adopt a 'no-fault' approach by prioritizing industry engagement, education, and the training and simulation of cybersecurity attacks. By fostering a culture of continuous learning and resilience, the CIRB enables organizations to openly share their experiences and collectively address cybersecurity challenges, ultimately enhancing the overall security posture of the industry.

23. What factors would make a cyber incident worth reviewing by a CIRB?
A cyber incident would merit review by a CIRB based on several key factors that contribute to the enrichment of cybersecurity knowledge and the enhancement of defense strategies across the community:

1. **Novelty:** Incidents involving unprecedented or innovative cyber threats that have the potential to provide new insights into attacker methodologies or emerging trends. By examining novel threats, the CIRB can contribute to the identification and mitigation of evolving cyber risks.

2. **New Attack Methods:** Incidents that demonstrate previously unknown or significantly evolved attack vectors, techniques, tactics, and procedures (TTPs) that expand the collective understanding of cyber threats. By analyzing new attack methods, the CIRB can inform the development of more effective defense strategies and countermeasures.

3. **Community Value:** Incidents whose analysis and lessons learned could greatly benefit the wider cybersecurity community by enhancing preparedness and response strategies. By focusing on incidents with significant community value, the CIRB can prioritize resources and efforts to address critical cybersecurity challenges and vulnerabilities.

4. **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. By leveraging incidents with educational potential, the CIRB can contribute to the professional development of cybersecurity practitioners and the cultivation of a skilled workforce.

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. By prioritizing incidents based on their novelty, impact, and educational value, the CIRB can fulfill its mandate of promoting continuous learning and resilience within the cybersecurity ecosystem.

24. Who should be a member of a CIRB? How should these members be appointed?
Members of a CIRB should be carefully selected to include individuals from academia and organizations specializing in cybersecurity training. This diverse composition ensures that the board benefits from a strong focus on education and possesses the necessary expertise to effectively train cyber defenders.

To appoint these members, a structured nomination process should be implemented to ensure transparency, fairness, and inclusivity. This process could involve the following steps:

- **Open Nominations:** Relevant organizations and educational institutions should be invited to nominate candidates who have demonstrated expertise and commitment to cybersecurity education and defense training. Open nominations encourage broad participation and allow for the identification of highly qualified candidates from various sectors of the cybersecurity community.

- **Peer Review:** Candidates' qualifications and contributions to the cybersecurity field should be rigorously assessed by a committee of their peers. Peer review ensures that selected members have earned the respect and recognition of the cybersecurity community through their expertise, experience, and contributions. This step helps maintain the integrity and credibility of the CIRB.

- **Diverse Representation:** Efforts should be made to ensure that the board includes a diverse range of expertise, encompassing different areas of cybersecurity. This diversity ensures a holistic approach to incident review and educational content development, incorporating insights from various disciplines and perspectives within the cybersecurity field.

By following such a selection process, the CIRB can ensure that its members possess the requisite knowledge, experience, and credibility to fulfill their responsibilities effectively. Additionally, this approach fosters a culture of inclusivity and collaboration within the cybersecurity education and training community, promoting the development of robust incident response capabilities and the continuous improvement of cybersecurity practices.