Australian cyber security strategy: Legislative reforms submissions from Notion Digital Forensics

OK FOR RELEASE

1 March 2024

Prepared By	Mr Matthew O'Kane B. Sc. BIT (Hons I), MBA, Masters of Cyber Security
Address:	Suite 34 Mezzanine 388 George St Sydney NSW 2000 Australia
Email:	[redacted]
Notion Project ID:	2024-AAW-P01
Notion Document ID:	2024-AAW-R01

Table of Contents

Summary of this document 4
Summary of the consultation response 4
Measure 2: Ransomware reporting 4
Measure 4: Cyber Incident Review Board 5
Notes about this analysis 6
My objective is to improve Australian cyber resilience 6
Limitations 6
Not legal advice 6
Written on behalf of Notion Digital Forensics 6
No payment means advice is provided 'as is' 7
Expert's Certificate 7
Conventions 8
Assumptions 9
Measure 2: Ransomware reporting for businesses 10
Summary of the proposal from the government 10
Insights on the proposed ransomware reporting framework 10
Evaluating the proposed reporting regime 12
Strategic information sharing to fight, not foster, crime 12
League tables – avoiding closer relationships with criminals 13
Sunset provisions to drive increased cyber defence efforts 13
Correcting public perception that ransomware strikes are 'sophisticated' 14
Recommendations for a balanced and effective reporting framework 14
Measure 4: Learning lessons after cyber incidents – A Cyber Incident Review Board 16
Summary of the proposal from the government 16
Input on the proposed Cyber Incident Review Board (CIRB) 17
The objective and culture of the CIRB 17
Enhancing national cyber resilience 17
Audience and accessibility: reports in plain English 17
Evidence collection and legal considerations 19
Membership composition and appointment 20
No need for security clearances 20

Reviews should broadly represent the range of cyber crimes suffered 21
Addressing a wide range of cyber threats 21

Summary of this document

Summary of the consultation response

1. This response is provided by Notion Digital Forensics to the "2023-2030 Australian Cyber Security Legislative Reforms Consultation Paper" from the Department of Home Affairs.

2. I focus on Measures 2 (Ransomware Reporting) and 4 (Cyber Incident Review Board), based on my specialised experience in cyber emergency response and digital forensics.

Measure 2: Ransomware reporting

3. Our main aim should be to help Australians stop ransomware attacks. If that fails, we should focus on lessening their damage.

4. An essential strategy is to discourage ransom payments to make such crimes less attractive, protecting Australian businesses and individuals.

5. The government's seeks to collect two pieces of data:

    a. Ransom demands, and;

    b. Ransom payments.

6. While intended to increase compliance in collecting data, the "no liability" clause for reporting payments needs careful consideration to avoid unintended negative outcomes.

7. I suggest improvements in this submission to achieve our aim of stopping ransomware attacks.

8. I suggest making protections for reporting ransom payments temporary. This is because many ransomware attacks can be stopped with simple cyber security measures. By sharing this information with the Australian public and setting a time

limit on 'no liability' for reporting ransom payments, we can encourage a stronger approach to cyber defence.

Measure 4: Cyber Incident Review Board

9. The Cyber Incident Review Board proposal is a positive step towards improving Australia's cyber resilience. My suggestions for its success include:

   a. Reviewing a wide range of cyber attacks, not just significant ones, to reflect the varied experiences of Australian organisations.

   b. Prioritising openness and transparency to spread cyber resilience knowledge as widely as possible, and making reports easy to read and access.

   c. Protecting ongoing investigations and intelligence work.

   d. Selecting CIRB members with diverse experiences, including those skilled in dealing with victims and without security clearances, drawing on the justice system's existing protocols for managing sensitive information.

   e. Developing strategies to prevent problems with evidence and ensure cooperation from all involved.

10. These recommendations aim to position the CIRB as a trusted component in strengthening Australia's approach to cyber security, guiding effective policy, and building a culture of resilience against cyber threats.

11. This summary is not a substitute for my full submission.

Notes about this analysis

My objective is to improve Australian cyber resilience

12. The Australian Department of Home Affairs seeks submissions on proposed changes to the way officials deal with cyber security in Australia. In summary, the measures I address in my submission deal with the following matters from the government's consultation paper.

    a. Part 1, Measure 2: Ransomware reporting for business[1]

    b. Part 1, Measure 4: Learning lessons from cyber incidents - the Cyber Incident Review Board[2]

13. My objective in writing these submission is to use my direct knowledge as a cyber emergency responder to provide guidance to policy, that improves the cyber resilience of Australia.

Limitations

Not legal advice

14. To avoid doubt, this document offers no legal opinions or advice.

Written on behalf of Notion Digital Forensics

15. Although I write this submission in the first person (as is the practice for incident reports used in the justice system), I am writing on behalf of Notion Digital Forensics, which is a business owned by Quatara Consulting Pty Ltd (Australian Business Number 69 103 224 380). Any opinions in this report are attributable to Notion Digital Forensics.

[1] pp13-17; 2023-2030 Australian Cyber Security Legislative Reforms Consultation Paper
[2] pp22-29; ibid

No payment means advice is provided 'as is'

16. At this time, there is no service agreement between Notion Digital Forensics and the Department of Home Affairs, Australia. Therefore, advice given is general and may not be suitable for your situation. Advice has also not undergone the company's normal rigorous fact checking, verification, and review process. To avoid doubt, this submission does not contain advice you should rely upon without first signing a service agreement with Notion Digital Forensics or seeking alternative professional input. This work is unpaid and is 'as is' and without warranty of any kind.

Expert's Certificate

17. I am qualified to provide an opinion on matters in this submission because:

    a. **Professional experience in digital forensics and incident response**: I am the owner of a digital forensics and incident response (DFIR) company, leading numerous investigations for commercial entities, Information Technology (IT) companies, law firms, and individuals. This demonstrates my hands-on experience and direct knowledge of cyber investigations and emergency response, enabling me to provide expert insights into the intricacies of these processes.

    b. **Courtroom validation of expertise**: My investigative work has been rigorously examined and validated in litigation. This validates the clarity and quality of my reports, confirming they are comprehensible to a broad audience and uphold high standards.

    c. **Educational background in information technology**: I earned a Bachelor of Science with First Class Honours in Business Information Technology from the University of New South Wales in 1999. This shows my formal understanding of both technical and non-technical areas of information technology, and that knowledge has evolved over a long time period.

    d. **Advanced qualifications in cyber security and digital forensics**: In 2023, I was awarded a Master of Cyber Security, majoring in digital

forensics, by UNSW Canberra. This highlights my advanced formal education in digital forensics, ensuring my knowledge is both current and specialised in fields directly relevant to this submission.

e. **Extensive career in technical and management roles:** For over twenty five years, I have occupied various technical and management positions related to software development, computer systems support, and maintenance. This experience underscores my practical understanding of how computer systems are developed, operated, and maintained.

f. **Academic contributions to cyber security education**: I am a casual academic at both UNSW Canberra and UNSW Sydney, where I design courses, assess student work, and lecture in cyber security and digital evidence. This is important because it shows my expertise is high enough to train the next generation of cyber defenders, business leaders and lawyers.

g. More details on my career history can be found on my public LinkedIn profile: `https://www.linkedin.com/in/australianinternetconsultant/`

Conventions

18. When I discuss cybercrime, I'm referring to any kind of unauthorised attack on civilian businesses or people that subverts their computer systems' confidentiality, integrity, trustworthiness, or availability. These attacks can come in various forms, like hacking, scams, or other tricks (among others).

19. In this report, I make no distinction between a cyber attack coming from a criminal or a foreign official group. I refer to them both as crimes for this submission.

20. I won't be talking about situations where one government is attacking another in cyberspace. That's not my area of expertise, so I won't go into that in this report. I'm focusing on attacks against civilian businesses and people in this submission.

Assumptions

21. The proposed "no liability" provision in Measure 2 (as found on page 16 of the consultation paper) **may** lead to a perceived decriminalisation of ransom payments. The consultation paper duly notes the absence of an outright ban on ransom payments, but this comment does not fully capture the complexities of the existing legal framework.

22. If the government provides assurances that could be misconstrued as protection from prosecution for a ransom payment, it might signal a shift towards non-enforcement, which could be interpreted as an effective decriminalisation of such payments.

Measure 2: Ransomware reporting for businesses

Summary of the proposal from the government

23. From the government's discussion paper, Measure 2 is summarised thus (page 13):

> - Ransomware and cyber extortion incidents pose some of the most significant and destructive cybercrime threats to Australian individuals and organisations. Ransomware uses malicious software to cripple digital infrastructure by encrypting devices, folders and files, rendering essential computer systems inaccessible unless a ransom is paid. Cyber extortion occurs where cybercriminals exfiltrate commercially sensitive or personal data from victims, threatening sale or release if extortion demands are not met.
> - Limited visibility of the ransomware and cyber extortion threat restricts the capacity of the government and private sector to help Australian organisations prepare for, and respond to, these incidents. Timely reporting of ransomware and cyber extortion incidents would accelerate law enforcement action, enhance whole-of-economy risk mitigation and help tailor victim support services.

24. Notable suggestions for the proposal include:

a. Reporting ransomware demands,

b. Reporting ransom payments,

c. A 72 hour timeframe for reporting.

Insights on the proposed ransomware reporting framework

Notion's starting position – ransom payments are bad for Australia

25. Paying ransoms is bad for everyone in Australia. This is my starting position in this analysis.

26. There might be a very rare situation where paying a ransom could be considered. By way of fictious example, I could not see an Australian jury convicting someone for paying a ransom to save a person's life.

27. Clearly such judgments exist on a continuum about what is a reasonable response to a ransom demand[3]. This is not a paper to explore such things, and the law is untested[4] in this area within Australia. Lawyers, government and companies have differing opinions[5] [6] on the current legality of ransom payments. However, much writing agrees that there is (or should be) defences to making payments based on the circumstance. It seems reasonable to argue such circumstances should mean ransom payments are rare and only in exceptional circumstances.

28. If it is true that ransom payments are widespread[7], then clearly legal advisors are reaching the view that they are OK to make payments.

29. But even if it's sometimes legal, paying ransoms just gives money to criminals and makes things worse for all of us. It encourages criminals to keep doing what they're doing and even aim for more targets.

---

[3] In Gunning, P: "Cyber attacks: is it legal to pay a ransom in Australia?" (7 July 2020), Mr Gunning sets out the defence of 'duress' in the legislation for funding criminals or terrorists. From Section 10.2, Criminal Code Act 1995 (Cth), "Duress will be made out if a person reasonably believes that: a) a threat will be carried out unless an offence is committed; b) there is no reasonable way the threat can be rendered ineffective; and c) the conduct or payment must be a reasonable response to the threat." Source: https://www.kwm.com/au/en/insights/latest-thinking/cyber-attacks-is-it-legal-to-pay-a-ransom-in-australia.html

[4] I do not know of anyone who has been prosecuted for paying a ransom in Australia, and I do not know of a case that seeks to more clearly define when the 'duress' defence is activated. Therefore, this area remains open to interpretation by lawyers.

[5] Shane Wright from the Sydney Morning Herald quoted Minister O'Neil on 13 November 2022: as saying "… making the payment of ransoms illegal was one of the options being considered"… Source: We will hunt them down: O'Neil signals more action on Medibank hack (smh.com.au)

[6] Melissa Tan, in February 2023 put the position that ransom payments are not illegal, but expressed concerns the government was considering making them illegal. She proposed reasonable defences for the payers of ransoms (such as necessity). Reference: Criminalising cyber extortion payments (landers.com.au)

[7] Purtell, James; 16 July 2021; ABC News; Australian organisations are quietly paying hackers millions in a 'tsunami of cyber crime'; https://www.abc.net.au/news/science/2021-07-16/australian-organisations-paying-millions-ransomware-hackers/100291542

30. Generally, the common wisdom is that paying a ransom can help one organisation but hurt everyone else by encouraging more crime. That's why we think it's important to avoid paying ransoms whenever possible.

31. So, our main rule is simple: don't pay ransoms. If there's an extreme case where it feels like the only option, it should be very rare and only for a very good reason.

Evaluating the proposed reporting regime

32. The government's proposal for a new way to report ransomware incidents is a significant move to strengthen our cybersecurity. These proposals are not yet law, but they bring up several important issues that need careful thought:

    a. **Concerns over normalising ransom payments:** The proposals might inadvertently make paying ransoms seem like an acceptable action[8], which could encourage more criminal activity.

    b. **Reduced urgency to bolster cyber defences**: There is a risk that businesses might focus more on responding to incidents through after-the-event ransom payments rather than improving their security measures before-the-event. In my experience, most ransomware attacks are easily defended against with basic cyber security controls. We should be encouraging businesses to do this.

    c. **Scope and scale of reporting obligations**: The proposal to exempt small businesses from reporting is sensible to reduce their burden. However, it's crucial to ensure this does not weaken our overall cybersecurity efforts.

Strategic information sharing to fight, not foster, crime

33. Collecting information about ransom payments such information opens the door to an outcome I call 'league tables' which could encourage some commercial providers to build relationships with criminals. They may advertise to the community

[8] p16, "No fault' and 'no liability' protection principles, Consultation Papr

how reliable their outcomes are with criminal gangs, thereby normalising a laundered cash flow from the legitimate sector of the economy to criminals.

League tables – avoiding closer relationships with criminals

34. In the collection of this data, national defenders may see some commercial cyber security companies closing more ransoms than other companies.

35. Avoiding league tables of performance with criminals is crucial in discouraging businesses from forging closer relationships with criminal groups. That's because:

    a. Since ransom payments might temporarily benefit a particular business but ultimately compromise national cyber resilience, it's essential to resist any inclination to endorse individuals or entities with established, trustworthy connections to criminal networks. Such endorsements could inadvertently formalise business relationships with criminal organisations, undermining our collective cybersecurity efforts and ethical standards.

    b. Such rankings could tempt government officials to favour/recommend private incident responders who have established relationships with criminal gangs over more ethical companies. This could undermine the integrity of our crime fighting efforts and encourage questionable practices.

36. If this data is to be collected, making sure this data helps everyone equally is key to maintaining a fair and effective cybersecurity environment. The data should not fall into the hands of a 'favoured few'.

Sunset provisions to drive increased cyber defence efforts

37. Sunset clauses are key to keeping the ransomware reporting rules up-to-date and effective, as well as encouraging Australian business to strengthen their cyber security stance in a timely manner.

38. Sunsetting also make sure that any unintentional protection given to companies reporting ransomware payments is only temporary. This nudges businesses to beef up their cyber defenses.

Correcting public perception that ransomware strikes are 'sophisticated'

39. In my work responding to ransomware emergencies, I've seen firsthand that many attacks could have been prevented by basic cybersecurity practices. Contrary to widespread belief, fueled by organizations claiming to be victims of 'sophisticated attacks', the truth is, most cyber breaches are not overly complex. My findings last year consistently showed that straightforward cyber security measures could have thwarted almost all of these ransomware incidents.

40. The misconception that attacks are highly sophisticated often deters the adoption of simple, effective cybersecurity measures. Herein lies the importance of sunset clauses. By transparently addressing the real nature of most ransomware attacks—which are typically not as complex as portrayed—we can highlight how easy it is to implement protective measures. This clarity can encourage businesses to strengthen their cyber defenses within a two-year timeframe (say), after which the temporary protections for reporting ransom payments would be phased out. Such an approach promotes an honest conversation with the public and encourages the uptake of critical cyber protections.

Recommendations for a balanced and effective reporting framework

41. Considering these points, we suggest a few key changes to make sure the proposed rules do more good than harm:

    a. **Clarify legal stances**: It's important to re-emphasise while ransom payments aren't always illegal, they should be considered only after all other options have been exhausted and with legal advice.

    b. **Enhance cyber resilience**: Encourage all businesses to strengthen their cybersecurity. The sunset provisions should ensure this remains 'top of mind'.

    c. **Transparent and equitable information sharing**: Push for a system where anonymised data is shared openly, so all businesses can learn and improve their defenses and not just a limited subset chosen by officials.

d. **Discouraging close criminal ties by avoiding league tables:** Avoiding league tables is crucial in discouraging businesses from forging closer relationships with criminal groups. Since ransom payments might temporarily benefit a particular business but ultimately compromise national security, it's essential to resist any inclination to endorse individuals or entities with established, trustworthy connections to criminal networks. Such endorsements could inadvertently formalize business relationships with criminal organizations, undermining our collective cybersecurity efforts and ethical standards..

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

Summary of the proposal from the government

42. From the government's discussion paper, Measure 4 is summarised thus (page 22):

> Recent high-profile cyber security incidents have highlighted that government, industry and the community must do more to learn lessons from cyber attacks. To stay ahead of the growing cyber threats across today's complex technology landscape, we need to invest time and resources to understand the vulnerabilities that led to the attack. We also need to examine the effectiveness of government and industry responses to cyber incidents. Once we've identified lessons learned from cyber attacks, we need to share them widely across industry and the broader community to ensure we are better prepared to respond in the future.
>
> As it stands, there is currently no national mechanism to review the root causes of cyber incidents and assess the effectiveness of post-incident response. There is no unified national approach to share lessons learned from cyber incidents. We need a mechanism that can disseminate clear, attributable and concrete recommendations to strengthen our collective cyber resilience. This mechanism needs to have a clear focus on developing and publicly issuing recommendations, as modelled in other sectors across the economy.

43. Notable suggestions for the proposal of a Cyber Incident Review Board (CIRB) include:

a. The objectives of the CIRB;

b. What investigatory powers it should have;

c. What it should investigate;

d. How it should select panel members

Input on the proposed Cyber Incident Review Board (CIRB)

The objective and culture of the CIRB

44. The government's consultation paper outlines an admirable goal for the Cyber Incident Review Board (CIRB), inspired by successful examples. For the CIRB to truly make a difference, its leadership must prioritise:

a. Cultivating a culture that values openness and continuous learning.

b. Demonstrating empathy towards victims of cyber incidents.

c. Committing to enhance cyber resilience across all Australian communities.

45. This strategy will distinguish the CIRB from other entities focused on cybercrime, earning trust from both the industry and the wider community.

Enhancing national cyber resilience

46. The CIRB has a significant opportunity to bolster Australia's cyber defenses through transparent investigations and sharing learnings. This not only improves national resilience but also fosters a culture of proactive cybersecurity practices.

Audience and accessibility: reports in plain English

47. For the Cyber Incident Review Board (CIRB) to effectively contribute to enhancing Australia's cyber resilience, its findings and reports must be accessible to a broad audience.

48. To that end, reports should follow the format similar to what is used in Federal court, as specified in the GPN-EXPT[9] practice note. Notably, reports should be in plain English, but with appropriate references to relevant technical evidence to permit a technical person to engage with aspects of the report. These references should also respect the need to maintain some operational security for certain national and official works.

49. The essence of making these reports available in plain English (with technical references where necessary) is about sharing with the community knowledge they can safeguard their organisation against cyber threats. Here's why accessibility matters for each stakeholder group:

    a. **Business leaders and owners**: Access to understandable reports helps them make informed decisions to protect their enterprises. They can implement or improve cyber security measures based on real-world examples of breaches and recommended practices.

    b. **IT professionals and cybersecurity experts**: While they might be comfortable with technical language, clear and well footnoted/annexed insights can aid in a deep understanding of new threats and defence strategies.

    c. **National and other official defenders**: Clear reports support these stakeholders in aligning national cyber defence strategies with the latest threat intelligence and mitigation techniques.

    d. **Cyber investigators and responders**: Accessibility ensures that those in the field, like myself, can easily share and discuss findings with a wider audience, including those not specialised in cyber security, thereby fostering a community-wide protective ethos.

    e. **Legal professionals**: Plain English reports can aid in the evolution of cyber law, the pursuit of justice for victims, and the development of policies that further national cyber security interests.

[9] Justice Allsop, Expert Evidence Practice Note (GPN-EXPT), Federal Court of Australia, October 2017. Reference: https://www.fedcourt.gov.au/law-and-practice/practice-documents/practice-notes/gpn-expt

f. **Programmers and developers**: Understanding the vulnerabilities exploited in past incidents can inform safer coding practices and software development, reducing the risk of future breaches.

g. **Teachers and students across high school, vocational, and university:** Making cyber security knowledge accessible to students prepares the next generation to be more cyber aware and capable of contributing to Australia's cyber defence.

50. By ensuring CIRB reports are comprehensible and actionable to these diverse groups, we not only broaden the impact of each report but also cultivate a more cyber-resilient Australia. The strategy behind this approach is to demystify cyber security, making it a collective endeavour rather than the sole province of experts. This inclusive perspective is crucial for building a nationwide culture of cyber awareness and resilience.

Evidence collection and legal considerations

51. Collecting evidence presents its challenges, and while a detailed legal framework is beyond this submission's scope, starting points for such an analysis could include:

a. Ensuring CIRB investigators adhere to established expert witness guidelines (eg GPN-EXPT), thus guaranteeing evidence is relevant, impartial, and clearly presented.

b. Mandating truthful evidence provision, with considerations for misleading or incorrectly handled information, which is often encountered in digital forensic investigations.

c. Gathering evidence from foreign entities can be complex due to legal and operational barriers. This is particularly true when dealing with global tech giants, underscoring the need for careful consideration in the CIRB's approach.

Membership composition and appointment

52. A crucial aspect of the CIRB's success lies in its membership diversity. Unlike the model used in the United States, which predominantly features government and large corporate representatives[10], the CIRB should embrace a more inclusive approach. This diversity should encompass:

    a. Individuals with experience in the open justice system, skilled in articulating complex issues to varied audiences.

    b. Members who have provided support to victims of cyber incidents, offering invaluable insights into the human aspect of cyber attacks.

    c. Experts with a broad understanding of cyber challenges, including those beyond mere software breaches, to offer a comprehensive perspective on cybersecurity.

53. Such diversity will increase the credibility of the CIRB, and show that it is relevant to Australia's interest, not just 'the big end of town'.

No need for security clearances

54. Insisting on security clearances for CIRB membership could inadvertently limit the board's scope and effectiveness. Security clearances tend to bias a group towards a defence or government perspective, potentially sidelining valuable insights from the business sector and the wider community. Such a requirement might also deter skilled professionals who work outside of government and defence sectors but possess critical expertise in cyber security and victim support.

55. Moreover, an open and transparent board, unencumbered by the need for security clearances, is more likely to engender public trust. Trust is the cornerstone of effective public engagement in cyber security practices.

56. The justice system already demonstrates that sensitive information can be handled effectively without necessitating security clearances for all involved. By adopting a similar approach, the CIRB can ensure that its membership is as diverse and

[10] Source: https://www.cisa.gov/cyber-safety-review-board-csrb-members

inclusive as possible, enhancing its capacity to address a wide range of cyber issues.

Reviews should broadly represent the range of cyber crimes suffered

57. The CIRB should not only focus on major cyber incidents but also on those that provide insights into common vulnerabilities and can significantly impact national resilience. Expanding the focus to include a variety of incidents will enrich the learning outcomes for all Australians.

Addressing a wide range of cyber threats

58. Contrary to popular belief, not all cyber attacks involve sophisticated hacking. Many, including ransomware and invoice fraud, can be prevented with basic measures. The CIRB's exploration of these and other incidents, such as competitive sabotage, will demonstrate the broad nature of cyber threats and the straightforward steps available to mitigate them, reinforcing the need for comprehensive cybersecurity strategies.

The above 58 paragraphs are my submission in response to "2023-2030 Australian Cyber Security Strategy: Legislative Reforms" written by the Department of Home Affairs.

Matt O'Kane
Director
Notion Digital Forensics, Sydney Australia