NOTION DIGITAL
FORENSICS

Submission to the Committee reviewing the Cyber Security Legislative Package 2024

25 October 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-R02b

Table of Contents

Summary of this document

1. As a follow-up to my March 1, 2024 submission on the Australian cyber security strategy, I welcome the opportunity to provide additional input on the Cyber Security Bill 2024. I am particularly encouraged to see that the draft legislation has incorporated my earlier recommendations regarding the Cyber Incident Review Board.

Ransomware Reporting Framework

2. My central position is that Australia's ransomware strategy should focus first on prevention, and then on damage mitigation when attacks occur. To achieve this, I recommend:

    a. **Data sharing for collective defence:** The Australian community needs to make ransomware less profitable for criminals. While the current legislation offers legal protection for organisations that report ransomware incidents, this protection should come with reciprocal benefits for the broader community. Specifically, I propose that organisations receiving legal protection should contribute to publicly aggregated data so we can measure the effectiveness of our cyber defences.

    b. **Safeguards to prevent unintended outcomes:** I recommend implementing:

        i. A framework for sharing trend data while protecting sensitive details

        ii. Clear boundaries to prevent legitimising relationships with criminal groups (detailed later in the submission)

        iii. A sunset clause for legal protections to encourage proactive security investments rather than reactive ransom payments.

Cyber Incident Review Board Enhancements

3. The proposed Cyber Incident Review Board represents a significant step forward for Australia's cybersecurity landscape. I acknowledge and appreciate that the draft legislation has already incorporated two key recommendations from my previous submission:

    a. The requirement for reviews to cover a diverse range of cyber incidents

    b. The inclusion of board members beyond those with security clearances, enabling broader industry participation

4. To further strengthen the proposed CIRB concept, I recommend:

    a. Including government data breaches that don't involve national security issues in the board's scope. This would demonstrate the public sector's commitment to transparency and shared learning.

    b. Expanding membership criteria to ensure representation from professionals with direct front-line incident response experience.

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

Notes about this analysis

My objective is to improve Australian cyber resilience

6. The Parliamentary Joint Committee on Intelligence and Security 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 draft legislation.

    a. Part 4: Ransomware reporting for business

    b. Part 6: Learning lessons from cyber incidents - the Cyber Incident Review Board

7. 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

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

Written on behalf of Notion Digital Forensics

9. Although I write this submission in the first person (as is the practice for expert's reports), 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.

Expert's Certificate

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

a. **Academic contributions to cyber security education**: I am a lecturer and assessor for UNSW Canberra's subject ZEIT8028 – Digital Forensics taught as part of the Master of Cyber Security Course. Further, 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.

b. **Professional experience in digital forensics and incident response**: I am the owner of a digital forensics and incident response (DFIR) company, leading 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.

c. **Validation of expertise in litigation**: 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.

d. **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.

e. **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 validates my formal education in digital forensics, ensuring my knowledge is both current and specialised in fields directly relevant to this submission.

f. **Career in technical and management roles:** For over twenty five years, I have performed various technical and management positions related to

software development, computer systems support, and maintenance. This experience demonstrates my practical understanding of how computer systems are developed, operated, and maintained in business.

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

Conventions

11. 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).

12. 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.

13. 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 my area of expertise only, which is attacks against civilian businesses and people in this submission.

Assumptions

14. The proposed "no liability" provision in Section 29, 30, 31 and 32 **may** lead to a perceived decriminalisation of ransom payments. That is because 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.

Part 3: Ransomware reporting for businesses

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

Recap of March 2024 submission on the ransomware reporting rules

15. I amplify and re-emphasise my submission from March 2024, which said (in part):

> *MOK* *Paying ransoms is bad for everyone in Australia. This is my starting position in this analysis.*
>
> *There might be rare situations 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.*
>
> *Clearly such judgments exist on a continuum about what is a reasonable response to a ransom demand[1]. This is not a paper to explore such things, and the law is untested[2] in this area within Australia. Lawyers, government and companies have differing opinions[3] [4] 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.*

[1] 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

[2] 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.

[3] 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)

[4] 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)

> *If it is true that ransom payments are widespread[5], then clearly legal advisors are reaching the view that they are OK to make payments.*

16. While the legal status of ransom payments remains debatable, their negative impact on Australia's cyber resilience is clear. Each payment, regardless of its legality, provides criminals with both funding and validation of their business model. This perpetuates a cycle of criminality that undermines our national cyber defence efforts and puts more Australian organisations at risk.

17. While I maintain this position, I recognise the value in gathering and sharing accurate data about extortion trends. If this policy experiment should proceed, I offer specific recommendations to maximise its value to society.

18. In exchange for granting such a significant concession, the Australian people should expect both measurable progress towards crime reduction and strong safeguards against normalising criminal behaviour.

Ambiguity over the "safe harbour" provision

The effect could likely result in a safe harbour with the currently drafted legislation

19. The draft legislation presents an apparent contradiction:

    a. The notes for Section 32[6] explicitly state the legislation is not intended to create a 'safe harbour' for ransom payments

    b. However, Section 32(2) prohibits using ransomware reports as evidence in investigating or prosecuting illegal ransom payments

20. This creates a practical enforcement paradox:

[5] 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

[6] Paragraph 261 of https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fems%2Fr7250_ems_2474a1f7-f1f0-4895-9113-3b8532da3377%22

a. The departments receiving protected ransom reports are typically the same ones responsible for investigating potentially illegal payments (if such things were investigated)

b. Without the ability to use reported information, these departments would lack crucial evidence for enforcement actions

c. This effectively creates an unintended safe harbour, despite the stated intention.

21. If the government cannot use the report of a ransom payment to investigate a potentially problematic payment, then payers will not be prosecuted[7]. This will result in the effective decriminalisation of ransom payments via this safe harbour.

a. If the intention is to create a safe harbour (to increase the chance of reporting), then I propose removing the ambiguity from the legislation. This ambiguity could force cyber responders or victims of crime to seek specialised legal advice.

b. If the intention is not to have a safe harbour, then I would suggest providing clarity on the existing laws regarding ransom and defences fro payments, with examples, so as not to have to necessitate obtaining complex and specialised legal advice during a cyber emergency event.

Society should receive benefits in return for concessions on ransom payments

22. If policy makers choose to effectively decriminalise ransom payments through safe harbour provisions, this significant concession should deliver clear public benefits:

a. Implement mandatory public reporting of aggregated data

b. Track and publish trends in:

i. Ransom demands

ii. Payment frequencies

iii. Payment amounts

[7] Note, there should remain the defence of duress, because sometimes paying is the only choice.

iv. Related crime statistics

Strategic information sharing: balancing transparency with security

23. My March submission's concerns about information security may have been interpreted as advocating complete secrecy. This was not my intent. Rather, I support sharing aggregated information with all stakeholders while preventing incentives that could encourage closer ties with criminal groups.

24. From my March submission, I identified two key risks to manage:

    a. The potential emergence of informal 'league tables,' where a small group of APS staff and contractors could identify which companies facilitate the most successful ransom payments. This could inadvertently encourage referrals to law firms or cyber response companies based on their ability to negotiate with criminal groups.

    b. The risk of normalising relationships with criminal groups. If we effectively decriminalise ransom payments, some parts of the cyber incident response ecosystem might develop ongoing relationships with criminal actors.

25. To address the 'league table' risk, I propose removing Section 27, Part 2(F) (regarding "communications with the extorting party") from the legislation. Making this information uncollectable would help prevent tracking of successful extortion transactions, reducing the risk of informal league tables developing.

26. To enable effective oversight, I propose expanding Section 27, Part 2 to require reporting of which cyber insurance companies, law firms, and incident response companies are involved in each case. This would help authorities identify concerning patterns in ransom payments while considering the complexity and context of different incidents.

Sunset provisions to drive increased cyber defence efforts

27. I re-amplify my position from March, which the most important part was:

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.

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 defences.

Correcting public perception that ransomware strikes are 'sophisticated'

In my work responding to ransomware emergencies, I've seen firsthand that many attacks could have been prevented by way of applying commonly accepted cybersecurity practices. Contrary to widespread belief, fueled by organisations claiming to be victims of 'sophisticated attacks', the truth is, many 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.

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 defences 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.

Part 5: Learning lessons after cyber incidents – A Cyber Incident Review Board

Government leadership in cyber incident reviews

28. The Australian government has an opportunity to demonstrate leadership through transparency in cyber incident management. While certain breaches must remain confidential due to national security implications or ongoing investigations, many government incidents could benefit from open review and shared learning.

29. This view is supported by recent data from the Office of the Australian Information Commissioner, which recorded[8] 63 breach reports from Australian government entities between January and June 2024. It seems reasonable to conclude that not all these incidents involved sensitive national security matters. Including appropriate government breaches in the review process would:

    a. Demonstrate the public sector's commitment to transparency

    b. Share valuable lessons across both public and private sectors

    c. Build public confidence in government cyber security efforts

    d. Create opportunities for collaborative improvement

Incorporating front-line expertise in the CIRB

30. The effectiveness of the Cyber Incident Review Board would be enhanced by including members with direct front-line incident response experience. These practitioners regularly work with cyber crime victims across our community and understand the practical challenges organisations face during incidents.

[8] Notifiable Data Breaches Report: January to June 2024 | OAIC - https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-january-to-june-2024

31. Their hands-on experience would bring valuable insights to the Board's work by:

    a. Providing real-world context about how incidents unfold

    b. Understanding victims' immediate needs and challenges

    c. Bringing practical knowledge of what works - and what doesn't - during incident response.

The above 31 paragraphs are my submission to the committee on the proposed Cyber Security Bill.

Matt O'Kane
Director
Notion Digital Forensics, Sydney Australia