2023-2030 Australian Cyber Security Strategy: A Discussion Paper Response

Elinya L. Dyer

Supervisors: Dr Pei-Wei Tsai, Dr Jun Zhang

The School of Science, Computing and Engineering Technologies, Swinburne University of Technology

April 14, 2023

1 Introduction

This paper responds to the 2023-2030 Australian Cyber Security Strategy, by providing insights to posited questions, 2(d), 7, and 9, with empirical data that can be used to inform decision-making on ways forward for Australian Cybersecurity [9].

This submission was prepared by Elinya Dyer, a domestic undergraduate student studying a double degree in Computer Science (Cybersecurity) and Law, at Swinburne University of Technology. It was prepared under the supervision of Dr Pei-Wei Tasi, and Professor Jun Zhang, both of the School of Science, Computing and Engineering Technologies, at Swinburne University of Technology.

The submission builds on research completed for a summer project entitled "Policy and Cybersecurity Attack Tangling Trajectory Analysis", funded by the School of Science, Computing and Engineering Technologies, at Swinburne University of Technology.

Swinburne's cybersecurity community, led by Professor Jun Zhang, has significantly impacted cybersecurity education and research in recent years. For example, the Cyber Academy, in collaboration with Deloitte, aims to address the cybersecurity skills gap in Australia. This initiative has received an overwhelming response. We have introduced a new Bachelor of Cyber Security program to cater to the growing demand for cybersecurity professionals worldwide. Swinburne is proud to have hundreds of students with a focus on cybersecurity. We are also spearheading the Emerging Technologies graduation program, funded by the Australian government and designed to enhance Australian cybersecurity capabilities for digital transformation. Our esteemed faculty members, Prof. Yang Xiang and Prof. Jun Zhang, were recognised leaders in cybersecurity by The Australian in 2021 and 2020, respectively. The Australian also acknowledged Swinburne as the leading cybersecurity research institute in 2021.

2 Question 2(d). Should Australia consider a Cyber Security Act, and what should this include?

As of early 2023, Australia does not have a comprehensive and unifying cybersecurity act. The nation's cybersecurity legislation is dispersed across a myriad of legal domains, resulting in a fragmented regulatory landscape. At present, in the federal jurisdiction alone, multiple legislative instruments govern areas including data privacy, surveillance, infrastructure security, and cybercrime. The absence of a unifying cybersecurity act has prompted the government to introduce a patchwork of legislation, that has resulted in a splintered cyber legal environment.

The 2023 Australian Cybersecurity Strategy identifies that there may be a need for a compelling framework that introduces a single cohesive framework to guide how government and the general public should respond to looming cybersecurity challenges [9]. This unified framework could consolidate a bulk of laws under a single, cohesive umbrella, simplifying the compliance processes and ensuring a consistent approach to cybersecurity across various industries.

The challenge lies in determining the scope of this unified Act. There are many policy goals that should be worked for when implementing cybersecurity legislation, these include data protection and privacy, protecting critical assets, prevention, identification, and interference with cyber threats, and preventing cybercrime. Ideally, a Cybersecurity Act could replace existing legislation in all of these areas, including replacing existing legislation such as the Privacy Act, and the Security of Critical Infrastructure Act [1, 3].

Nonetheless, replacing the larger, stronger pieces of existing legislation through incorporation could potentially prove to be an unnecessary application of policy. A more strategic approach might be to focus the cybersecurity act on consolidating smaller, more nebulous cybersecurity protections currently dispersed across multiple pieces of legislation. This would not only enhance the efficiency of the legal framework but also promote a more coherent and unified system for addressing cybersecurity concerns.

It would be highly beneficial for the Cybersecurity Act to strive for future-proofing. The field is inherently complex, and determining the relevance of various technology-related laws involves navigating gray areas, particularly where emerging technology is concerned. To ensure the Act's longevity, it should carefully consider emerging technologies and their potential implications on cybersecurity. This includes forward-thinking on how to address challenges of the future including issues related to artificial intelligence, and quantum computing, which could significantly impact the cybersecurity landscape down the line. By including provisions that are able to cope with emerging technologies, the Act could help to put Australia at the front of the cybersecurity legal landscape.

It is a good idea for Australian policymakers to work towards the implementation of a Cybersecurity Act that consolidates existing legislation, where necessary, and addresses the diverse challenges of cybersecurity across various sectors, while remaining adaptive

to emerging technologies and the ever-changing threat landscape.

3 Question 7. What can government do to improve information sharing with industry on cyber threats?

There is currently a dearth of high-quality Australian cyber-related data. This scarcity of data aligns with a broader, previously observed, pattern of limited publicly accessible cybersecurity data [6]. This lack of data hampers the efforts of cybersecurity researchers, preventing accurate analysis, and potentially leaving Australia more vulnerable to cyber threats.

A properly informed research community is crucial for developing effective strategies to protect the nation's digital infrastructure and assets. The lack of data was particularly evident when searching through Australian dataset databases, such as data.gov.au and researchdata.edu.au, which surprisingly often produced few to no results for keywords such as "cyber" and "cybersecurity".

Although it appears evident that government-funded Australian cybersecurity organisations, such as the Australian Cyber Security Centre (ACSC) and Data61 are generating cybersecurity datasets, these resources are not being made clearly accessible for broader analysis by the research community [4, 11]. Given that organisations like the ACSC collect high-quality data, and are able to provide snapshots of figures intermittently, making available primary datasets should be considered to allow appropriate researchers to understand the mechanistic causes of the breaches [4].

Currently, however, there are many limits on data accessibility. The reasons for this limited access may include concerns over privacy, national security, or the proprietary nature of the data, and balancing these concerns given the often covert nature of cyber may prove difficult. However, without transparency and data sharing, it becomes increasingly difficult for researchers to identify trends, vulnerabilities, and potential solutions for enhancing cybersecurity in Australia [8].

Providing effective analysis and insight into topics using data science methods requires high-quality input data. The Australian Code for the Responsible Conduct of Research guidelines outlines that research data should be made available unless ethical, privacy, or confidentiality concerns are apparent [10]. Although there are valid concerns over the security of cybersecurity data, more work should be done to improve information sharing by ensuring that cybersecurity data is safe to release.

To improve information sharing, it is recommended that improvements to cyber data collection and availability be made, as the scope of a solution cannot be understood without understanding the problem.

4 Question 9. Would expanding the existing regime for notification of cyber security incidents (e.g. to require mandatory reporting of ransomware or extortion demands) improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime type?

Enhancing the existing regime for notification of cybersecurity incidents could significantly improve public understanding of the nature and scale of threats present in the cyber landscape. Currently, in areas where mandatory reporting schemes are lacking, such as ransomware or extortion demands, the absence of reliable data hinders efforts to accurately assess and report on the scope of the problem. As a result, the public remains under-informed about the true extent of these issues.

Mandatory reporting schemes are designed to compel organisations to disclose specific incidents, such as data breaches and other cybersecurity events. These schemes have strengthened Australian cybersecurity legislation by encouraging organisations to adopt a more proactive approach. Introduced in 2017, the Notifiable Data Breach (NDB) mandatory reporting scheme has proven to be an important source of data breach information [2, 5], early similar observations have also been made for the Security of Critical Infrastructure mandatory reporting scheme [7]. Extending the regime to encompass mandatory reporting of incidents like ransomware and extortion demands could elevate public awareness and comprehension.

Key advantages of mandatory reporting schemes include enhanced transparency, the promotion of better security practices, and improved threat intelligence. Mandated disclosures foster increased organisational transparency, which in turn builds trust and accountability with clients. Further, mandatory disclosures incentivise organisations to implement superior security practices, thereby avoiding the financial and reputational costs often associated with disclosure situations. Notably, mandatory disclosures also contribute to better threat intelligence, as most qualifying incidents are reported.

An analysis of the NDB data reveals the effectiveness of mandatory reporting in enriching threat intelligence, as illustrated in figure 1. In the graph we see NDB data, plotted in orange, is orders of magnitude higher than publicly reported ransomware incidents, plotted in light blue. The disparity between these datasets can primarily be attributed to their collection methods. The ransomware dataset comprises only publicly available information, likely representing a small fraction of actual incidents. Conversely, due to mandatory reporting requirements, the NDB dataset encompasses a vast majority, if not all, of the data breaches that occurred within the specified time frame. Implementation of a mandatory disclosure program for ransomware attacks would likely result in a similar occurrence range to that observed in the NDB data.

These schemes supply authorities with accurate information on incident occurrences that would otherwise be challenging to obtain, facilitating the proper allocation of resources

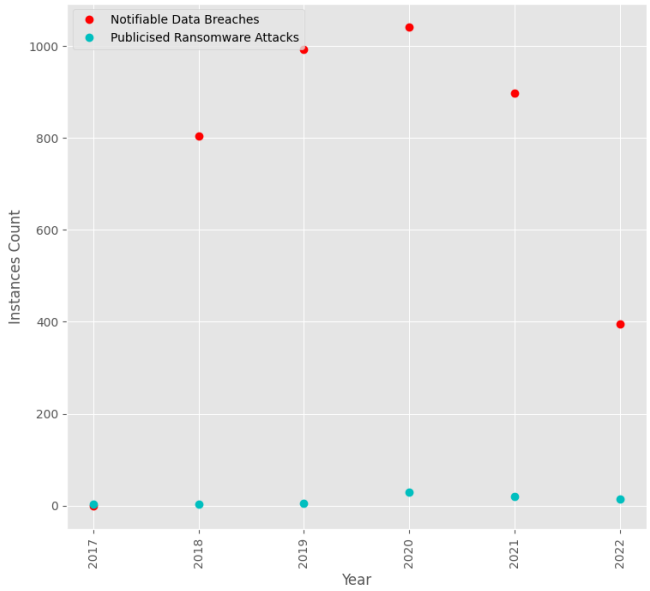

Figure 1: Australian NDB Data vs Publicised Ransomware Attack Data 2017-2022

and the development of targeted security strategies. By incorporating ransomware and extortion demands into the existing mandatory reporting framework, a better understanding of the prevalence and severity of these cybercrimes could be gained, improving transparency. This expansion would enable authorities and organisations to better comprehend the scale of the problem and drive more effective efforts to combat ransomware and extortion.

Other potential areas for expanding mandatory reporting could include vulnerabilities, Internet of Things (IoT) devices, cloud systems, and incidents involving critical assets. Addressing these areas would provide a more comprehensive view of the cybersecurity landscape, fostering a safer environment for businesses, individuals, and the Australian community. By improving public understanding and promoting collaboration among organisations and authorities, expanded mandatory reporting schemes have the potential to create a more resilient cybersecurity landscape in Australia.

References

[1] Privacy Act 1988 (Cth), 1988.

[2] Privacy Amendment (Notifiable Data Breaches) Act 2017, 2017.

[3] Security of Critical Infrastructure Act 2018 (Cth), 2018.

[4] Australian Cyber Security Centre. Annual cyber threat report, july 2021 – june 2022. Technical report, Australian Government, 2022.

[5] Asha Barbaschow. A whopping 890 data breach notifications were made to australia's privacy commissioner last year. *Gizmodo Australia*, Mar. 2023.

[6] Frank Cremer, Barry Sheehan, Michael Fortmann, Arash N. Kia, Martin Mullins, Finbarr Murphy, and Stefan Materne. Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva Papers on Risk and Insurance - Issues and Practice*, 47:689–736, 2022.

[7] Daniel Croft. 47 cyber incidents in critical infrastructure sectors reported in 9 months. Cybersecurity Connect, February 2023.

[8] Giuseppe Falco and et al. Cyber risk research impeded by disciplinary barriers. *Science (American Association for the Advancement of Science)*, 366(6469):1066–1069, 2019.

[9] Australian Goverment. 2023-2030 Australian Cyber Security Strategy, 2023.

[10] National Health and Medical Research Council, Australian Research Council, and Universities Australia. The Australian Code for the Responsible Conduct of Research, 2018.

[11] Benjamin Zhao, Muhammad Ikram, Hassan Asghar, Dali Kaafar, Abdelberi Chaabane, and Kanchana Thilakarathna. A decade of mal-activity reporting: A retrospective analysis of internet malicious activity blacklists. In *Proceedings of the 2019 APWG Symposium on Electronic Crime Research*, pages 193–205, 2019.