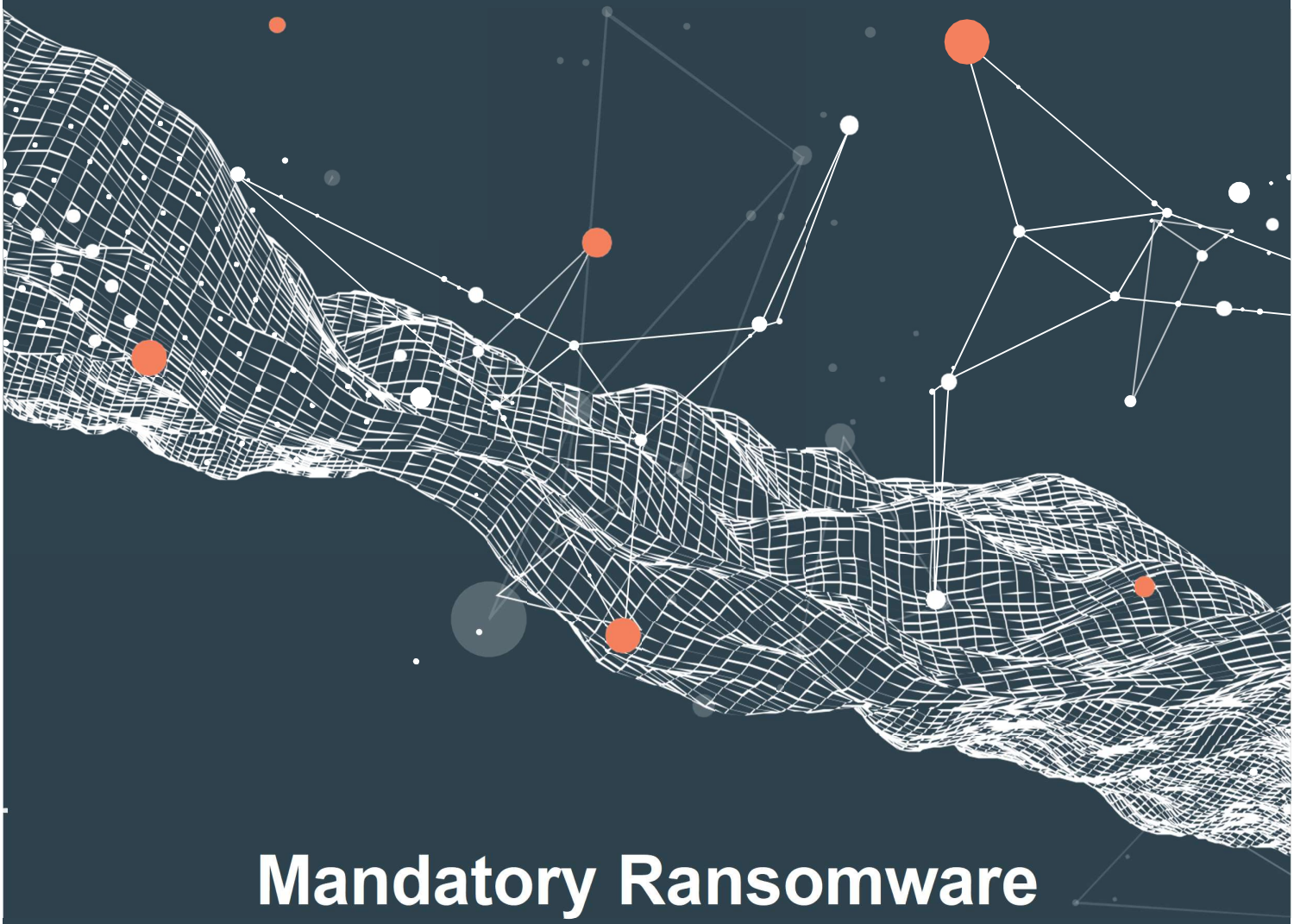
Australian Government

Department of Home Affairs



Mandatory Ransomware Payment Reporting – Cyber Security Bill 2024

Impact Analysis (OIA24-07090)

Contact us

Enquiries regarding the licence and any use of this document are welcome at:

Department of Home Affairs

PO Box 25

BELCONNEN ACT

2616 P - 23-02503-c

Contents

Executive summary

Ransomware remains the most destructive cybercrime threat to Australians and under-reporting limits Government's understanding of the extent of the problem and its ability to improve support to businesses in their response to ransomware threats. Under the *2023-2030 Australian Cyber Security Strategy*, the Australian Government has committed to disrupting the ransomware business model and preventing cybercriminals from profiting from attacks on Australian businesses and citizens. This includes working with industry to co-design options to legislate a no-fault, no-liability ransomware reporting obligation for businesses. This impact analysis considered four options available to introduce this measure:

- **Option 1:** Maintain the status quo
- **Option 2:** Encourage voluntary reporting of ransomware demands and payments
- **Option 3:** Legislate mandatory reporting of ransomware payments
- **Option 4:** Legislate mandatory reporting of ransomware demands and payments

For options 3 and 4, two thresholds to apply the reporting obligation were considered:

- **Option A:** Entities with an annual turnover of greater than $10 million
- **Option B:** Entities with an annual turnover of greater than $3 million

Option 3 was determined to present the best balance of regulatory impact and benefit as it would provide enhanced visibility of the ransomware threat, whilst limiting the reporting burden on businesses experiencing a cyber incident. Through consultation, a significant portion of stakeholders proposed Option 3 as striking the appropriate balance between these two things. Options 1 and 2 were not sufficient to address the lack of ransomware reporting as current voluntary reporting mechanisms have not been adequately utilised by industry. While Option 4 is sufficient for this need, this impact analysis concluded that the regulatory impact on industry was disproportionate for the additional benefit that double reporting would provide.

Option B was determined to present an appropriate threshold. This option captures approximately 6.56 per cent of registered Australian businesses (comprising roughly 50 per cent of the total annual turnover of all businesses in Australia) which is more than three times the number captured by Option A. This appropriately balances the impact on Australian businesses—particularly small businesses—while meeting the policy intent of building a clearer picture of the impacts of ransomware on the Australian economy. This threshold, supported by the majority of stakeholders, aligns with the *Privacy Act 1988*, where entities with an annual turnover of less than $3 million are considered to be small businesses and are generally exempt from reporting requirements for notifiable data breaches. A transition period of 6 months will be provided before enforcement of the new requirements takes effect to ensure that industry has adequate time to implement the reforms. This implementation timeframe was supported through consultation with industry.

Review of the measure will involve an assessment of whether the information collected is sufficient to inform relevant advisories to industry and whether any additional reform may be required.

The problem

Ransomware uses malicious software to cripple operations by encrypting devices, folders and files, rendering essential computer systems inaccessible unless a ransom is paid. Even if a ransom is paid, there is no assurance that data will be recovered or that data will not be on-sold or released. Similarly, in cyber extortion cases, cybercriminals extract commercially sensitive or personal data from victims, and threaten sale or release if extortion demands are not met.

Indicators show that cyber extortion is on the rise

Ransomware incidents pose some of the most significant cybercrime threats to Australian organisations, businesses and the community. Ransomware remained the most destructive cybercrime threat in 2022-23.[1] While ransomware comprised 10 per cent of all incidents the Australian Signals Directorate (ASD) responded to in this period, similar to 2021-22, ASD notified 158 entities of ransomware activity on their networks, compared to 148 in 2021-22, roughly a 7 per cent increase.[2] In addition to ransomware incidents themselves, the number of extortion-related cyber security incidents ASD responded to increased by around 8 per cent compared to the 2021-2022 financial year. In 2022-2023, ASD responded to 127 extortion-related incidents, 118 of these incidents involved ransomware or other forms of restriction to systems, files or accounts. Throughout this period, ASD reported that cybercriminals constantly evolved their tactics and operations to extract maximum payments from victims, fuelled by a global industry of access brokers, extortionists and ransomware-as-a-service operators.[3]

Ransomware threats impose a significant cost to the economy

Ransomware is deliberatively disruptive, and places pressure on victims by encrypting and denying access to files. Usually a ransom in the form of cryptocurrency is then demanded to restore access. This can cause severe disruption or even complete shutdown of operations for the many companies that are dependent on computer systems to operate and undertake core business functions. This can take weeks, and in some cases months, to recover from completely.[4] The United States Department of Homeland Security estimates that American businesses experience an average recovery period of 22 days.[5] The financial impact of ransomware is greater than the cost of lost production, sales or the price of the ransom itself. Additional expenses can include engaging digital forensic experts, investigations, communications, damage to brand reputation, on-going monitoring of systems, providing free credit or services and more.[6]

The true mean financial cost impact of ransomware is difficult to quantify, but has been variously estimated as:

- AUD6.77 million on average, from a survey in 2023 of 553 businesses globally (including 23 Australian firms).[7]
- AUD1.03 million on average for the ransom, excluding any other recovery costs and impacts, from a survey in 2023 of Australian businesses by McGrath Nicol. Respondents also noted they would be

---

[1] Australian Cyber Security Centre, *July 2022 to June 2023 Annual Cyber Threat Report*, Australian Signals Directorate, 2023, p 48 <https://www.cyber.gov.au/sites/default/files/2023-11/asd-cyber-threat-report-2023.pdf> ('ACSC Cyber Threat Report 2022-23').

[2] ACSC Cyber Threat Report 2022-23, p14.

[3] ACSC Cyber Threat Report 2022-23, p 11.

[4] Cohesity, *Global Cyber Resilience Report 2024*, 2024 <https://www.cohesity.com/resource-assets/research-reports/state-of-data-security-and-management-en.pdf>.

[5] Office of Intelligence and Analysis, *Homeland Threat Assessment 2024*, United States Department of Homeland Security, 13 September 2023, p 26 <https://www.dhs.gov/sites/default/files/2023-09/23_0913_ia_23-333-ia_u_homeland-threat-assessment-2024_508C_V6_13Sep23.pdf>.

[6] IBM, *Cost of a Data Breach Report 2023*, July 2023, p 15 <https://www.ibm.com/downloads/cas/E3G5JMBP> ('IBM Data Breach Report 2023').

[7] IBM Data Breach Report 2023, p 32. Note: the original reported value was USD4.54 million, and the conversion factor to AUD was provided at 1.4916.

willing to pay up to AUD1.32 million for a ransom payment.[8]

- USD2.6 million on average (USD750,000 median) for entities that paid a ransom, compared to USD1.62 million on average (USD375,000 median) for entities that did not pay a ransom, from a survey in 2023 by Sophos, which included up to 100 Australian respondents.[9]
- USD1.1 million for the average ransom payment excluding other recovery costs and impacts, as estimated by Crowdstrike.[10]
- More than USD1 Billion (AUD1.5 Billion in 2023) for total global ransomware payments, more than double its 2022, estimated by both Chainalysis and Sonicwall.[11] This does not include other losses businesses suffer, which can outweigh the cost of ransom.[12]
- USD381,980 for median ransomware payment, USD250,000 for mean ransomware payments from 2023, reported by Coveware[13]
- USD650,000 for median demand and USD350,000 for median payment in 2022, reported by PaloAlto[14]
- USD100,000 or more for average ransom payments and USD5.3 million average demand, was estimated by Zscaler[15]
- USD200,000 for average cost burden to companies, estimated by Cyfirma.[16]

There are many non-financial impacts attributable to ransomware and cyber extortion incidents. Cyfirma reported that 40 per cent of organisations downsize their workforce as a consequence of the financial strain caused by the incident. Additionally, in 35 per cent of affected organisations, C-suite members step down following the incident. Many smaller businesses experience existential threats to their operations, with 60 per cent of small businesses shutting down within six months following the attack.[17]

A quarter of the ransomware reports to ASD also involved confirmed data exfiltration, also known as 'double extortion'. This is where the actor extorts the victim for both data decryption and the non-publication of data. This proportion may be higher, but ASD note that it is difficult to validate exfiltration claims until the legitimacy of leaked data is confirmed.[18]

Recently, businesses that provide essential services, including critical infrastructure, education, legal and financial services entities, continued to be targeted, causing impacts on network operators and those relying on these essential services. For example:

- In May 2024 MediSecure, a national prescription delivery service provider, was subject to a suspected ransomware incident that involved data exfiltration affecting up to 12.9 million Australians.[19] Following the incident, MediSecure entered into administration.[20]
- In early 2023 HWL Ebsworth, a major Australian law firm, was subject to a ransomware attack that

---

[8] Darren Hopkins et al., *Ransomware: A Cost of Doing Business*, McGrathNicol, 2023, p 3 ('McGrathNicol Ransomware Report 2023') <https://a.storyblok.com/f/186891/x/4a4edc8426/mcgrathnicol_flyer-ransomware-survey-2023_v14.pdf>.

[9] Sophos, *State of Ransomware 2023*, May 2023, p 16 <https://assets.sophos.com/X24WTUEQ/at/c949g7693gsnjh9rb9gr8/sophos-state-of-ransomware-2023-wp.pdf> ('Sophos State of Ransomware Report 2023').

[10] VansonBourne, *2020 CrowdStrike Global Security Attitude Survey*, CrowdStrike, 2020, p 6 <https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CSGlobalSecurityAttitudeSurveyReport.pdf> ('CrowdStrike Global Security Survey 2020').

[11] Chainalysis Team, *Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline*, Chainalysis, 7 February 2024 <https://www.chainalysis.com/blog/ransomware-2024/>; Bob VanKirk, 2024 Sonicwall Cyber Threat Report, Sonicwall, 2024, p 7 <https://www.sonicwall.com/medialibrary/en/white-paper/2024-cyber-threat-report.pdf>.

[12] IBM Data Breach Report 2023, p 35.

[13] Coveware, *RaaS devs hurt their credibility by cheating affiliates in Q1 2024*, 17 April 2024, <https://www.coveware.com/blog/2024/4/17/raas-devs-hurt-their-credibility-by-cheating-affiliates-in-q1-2024> ('Coveware Blog').

[14] Wendi Whitmore, *Unit 42 Incident Response Report 2024*, Paloalto Networks, p 23 <https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report>.

[15] Zscaler, *Zscaler ThreatLabz 2023 Ransomware Report*, 2023, p 4 <https://www.zscaler.com/resources/industry-reports/2023-threatlabz-ransomware-report.pdf> ('Zscaler ThreatLabz Ransomware Report 2023').

[16] Cyfirma, Tracking Ransomware, February 2024 < https://www.cyfirma.com/research/tracking-ransomware-february-2024/> ('Cyfirma Tracking Ransomware 2024').

[17] Cyfirma Tracking Ransomware 2024.

[18] ACSC Cyber Threat Report 2022-23, p 48.

[19] Vaugh Strawbridge and Paul Harlond, *MediSecure statement on cyber security incident*, MediSecure Ltd, 18 July 2024 <https://medisecurenotification.wordpress.com/>.

[20] Department of Home Affairs, *MediSecure Cyber Security Incident*, 19 July 2024 <https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/cyber-coordinator/medisecure-cyber-security-incident>.

involved data exfiltration of sensitive customer records, including drivers licences, birth certificates and passports. Some Government agency data was exposed as part of the incident, due to HWL Ebsworth's contracts with various agencies. HWL Ebsworth advised that it did not pay the ransom.[21]

- In the first half of 2023 Latitude Financial, a major financial services provider, was subject to data exfiltration of several million personal records and other sensitive information,[22] and was subject to a cyber extortion demand which it did not pay.[23]
- In December 2022 Medibank, a major health insurance company, advised that a criminal had released personal data, including names, addresses, dates of birth and some passport numbers for sale on the dark web.[24] Some reports alleged that Medibank was subject to a $15 million (USD10 million) cyber extortion demand for over 9.7 million exfiltrated customer records,[25] which Medibank advised it would not pay.[26]
- In September 2022, the sensitive customer records, including passports, of over 10,000 customers of Optus, one of Australia's largest telecommunications providers, were compromised.27 A $1.5 million cyber extortion demand was made and subsequently retracted.[28]
- In late 2022, an Australian education institution was impacted by the Royal ransomware, compromising personal information of both students and staff.[29]
- Malwarebytes suggests that Australia suffers from roughly 2 per cent of all ransomware attacks globally,[30] and Zscaler reports that Australia receives 3 per cent.[31]

These trends are not just observed in Australia, but globally:

- In the latter half of 2022, the French health system reportedly sustained a number of cyber incidents. One hospital fell victim to a ransomware incident, resulting in the cancellation of some surgical operations and forcing patients to be transferred to other hospitals. The hospital's computer systems had to be shut down to isolate the attack.[32]
- In February 2023, an Italian energy and water provider was affected by ransomware. While there was no indication the water or energy supply was affected, it reportedly took 4 days to restore systems like information databases.[33]
- In February 2023, Dole – one of the world's largest producers and distributors of fruit and vegetables – was a victim of a ransomware incident, resulting in a shutdown of its systems throughout North America. Other reported impacts included some product shortages, a limited impact on operations, and theft of company data – including some employee information. While Dole acted swiftly to minimise the impacts of the incident, it still reported USD $10.5 million in direct costs, and faced reputational damage.[34]
- In January 2023, cybercriminals reportedly compromised the postal service in the UK, encrypting files and disrupting international shipments for weeks.[35]

---

[21] Australian Financial Review, *No deal: HWL Ebsworth will not pay ransom to Russia-linked hackers*, 9 June 2023 <https://www.afr.com/companies/professional-services/no-deal-hwl-ebsworth-will-not-pay-ransome-to-russia-linked-hackers-20230609-p5dfeg>.
[22] Latitude Financial, *Latitude Cyber Incident*, 2023 <https://www.latitudefinancial.com.au/latitude-cyber-incident/>.
[23] Latitude Financial, *Cybercrime Update 11*, 11 April 2023 <https://www.latitudefinancial.com.au/about-us/media-releases/cybercrime-update-11-04-2023.html>.
[24] Australian Cyber Security Centre, *Medibank Private Cyber Security Incident*, Australian Signals Directorate, 1 December 2022 <https://www.cyber.gov.au/about-us/alerts/medibank-private-cyber-security-incident>.
[25] ABC News, *Hackers claim they demanded $15 million ransom as more Medibank customer data posted to dark web*, 10 November 2022 <https://www.abc.net.au/news/2022-11-10/medibank-data-breach-latest/101637160>.
[26] Matthew Doran, *Medibank CEO says ransom amount 'irrelevant' and paying up would only increase risk of further extortion*, 7 November 2022 <https://www.abc.net.au/news/2022-11-07/medibank-ceo-says-ransom-amount-irrelevant-10-million-hacked/101625012>.
[27] Optus, *Latest updates & support on our cyber response*, September 2022 <https://www.optus.com.au/support/cyberresponse>.
[28] Australian Financial Review, *FBI called in, Optus hacker deletes data*, 27 September 2022 <https://www.afr.com/companies/telecommunications/more-optus-data-details-dumped-online-overnight-20220927-p5bl7s>.
[29] ACSC Cyber Threat Report 2022-23, p 48.
[30] Malwarebytes, 2024 State of Malware, May 2024, p 7 <https://go.malwarebytes.com/rs/805-USG-300/images/State-of-Malware-2024.pdf> ('Malwarebytes State of Malware Report 2024').
[31] Zscaler ThreatLabz Ransomware Report 2023, p 10.
[32] ACSC Cyber Threat Report 2022-23, p 27.
[33] ACSC Cyber Threat Report 2022-23 p 27.
[34] ACSC Cyber Threat Report 2022-23, p 21.
[35] ACSC Cyber Threat Report 2022-23, p 38.

Ransomware threats are significantly under-reported

The reporting of cyber incidents is primarily regulated for critical infrastructure and notifiable data breaches under the *Privacy Act 1988* that may relate to a cybercrime. The vast majority of businesses and other entities in Australia are not required to report cyber incidents. Furthermore, there is no existing reporting requirement for ransomware or cyber extortion payments. Australians can voluntarily report cyber incidents to law enforcement using ASD's Australian Cyber Security Centre's (ACSC) platform, ReportCyber. However, like many cybercrime and cybersecurity incidents, ransomware and cyber extortion attacks are underreported.

The extent of underreporting is difficult to estimate as there are no Government surveys on lack of reporting for businesses. The Australian Institute of Criminology indicates that, of members of the public who reported being a victim of ransomware, only one in five victims sought help, advice or support from either the police or ASD's ACSC.[36] Industry surveys and reports vary:

- 63 per cent of 553 businesses surveyed by IBM globally in 2023 opted to involve law enforcement in ransomware breaches.[37]
- 30 per cent of businesses surveyed by Ransomware.org globally in 2024 responded that law enforcement would be helpful during a ransomware incident.[38]
- 20 per cent of the victims of the Hive ransomware group reported being affected to the authorities in 2022, according to the United States Federal Bureau of Investigation.
- 15 per cent of cyber incidents are reported globally in 2023, according to BlackFog.[39]
- 60 per cent of 500 Australian businesses surveyed by McGrath Nicol in 2023 with more than 50 employees reported that it should be mandatory to report ransomware attacks to authorities, and 32 per cent sought reporting restricted to when a payment was made.[40]

There is also highly variable data on the proportion of businesses that would pay or have paid a ransom in relation to a cyber incident:

- 75 per cent of 280 Australian businesses that had been affected by a ransomware attack in the past five years surveyed by McGrath Nicol in 2023 advised that they paid a ransom demand within 48 hours of being impacted by a ransomware incident, with 70 per cent of 500 Australian businesses responding they would be willing to pay a ransom when faced with a high-pressure decision[41]
- 27 per cent of 2200 businesses surveyed by CrowdStrike globally in 2020 paid a ransom (around 200 respondents were Australian businesses).[42]
- 26 per cent of Australian organisations surveyed by Barracuda advised they would pay a ransom. Globally, 31 per cent of organisations paid a ransom when subject to a single attack, compared to 42 per cent for organisations that had been hit by three or more attacks.[43]
- 20 per cent of 2091 respondents from organisations globally surveyed by Thales in 2024 (including 108 Australian respondents) indicated that they had or would pay a ransom.[44]
- 54 per cent of IT professionals (including Australian) surveyed by Proofpoint advised that their organisation paid a ransom in 2023.[45]
- 53 per cent of 96 Australian organisations affected by cyber extortion that were surveyed by Sophos

---

[36] Isabella Voce and Anthony Morgan, *Help-seeking among Australian ransomware victims*, *Statistical Bulletin no. 38*, Australian Institute of Criminology, Canberra, 3 March 2022, pg. 5 <https://doi.org/10.52922/sb78504>.
[37] IBM Data Breach Report 2023, p 6.
[38] Ransomware.org, *The State of Ransomware 2024*, ActualTech Media, 2024, p 12 <https://ransomware.org/wp-content/uploads/2024/03/2024-State-of-Ransomware-Report_v1.pdf> ('Ransomware.org Report 2024').
[39] Brenda Robb, *The State of Ransomware 2024*, BlackFog, 1 August 2024 <https://www.blackfog.com/the-state-of-ransomware-2024/>.
[40] McGrathNicol Ransomware Report 2023, p 16.
[41] McGrathNicol Ransomware Report 2023, p 3.
[42] CrowdStrike Global Security Survey 2020, p 6.
[43] Barracuda, *2023 ransomware insights*, March 2023, p 8 <https://assets.barracuda.com/assets/docs/dms/2023-Ransomware-insights-report.pdf>.
[44] Thales, *2024 Data Threat Report*, March 2024, p 10 <https://www.thalesgroup.com/en/worldwide/security/press_release/2024-thales-data-threat-report-reveals-rise-ransomware-attacks>.
[45] Proofpoint, 2024 State of the Phish, February 2024, p 17 <https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-state-of-the-phish-2024.pdf>.

advised that they paid a ransom, compared to 46 per cent of 1497 businesses globally in 2022.[46]

- About 33 per cent of businesses negotiate ransomware payments, according to an interview with an alleged leader of ransomware-as-a-service operator REvil in 2020.[47]
- 71 per cent of businesses surveyed by Ransomware.org globally in 2024 indicated that they either would, or would consider, paying a ransom.[48]
- 76 per cent of 156 US businesses surveyed by Delinea in 2023 advised that they paid a ransom.[49]
- 48 per cent of 256 business leaders surveyed by Spycloud in 2023 whose organisations had been impacted by ransomware said that they had paid a ransom.[50]
- 38 per cent of 652 senior cybersecurity experts from companies with 1000 or more employees in the USA answered that they had a policy in place to pay a ransom, and 42% indicated they would pay a ransom, in response to a June 2023 survey by DeepInstict.[51]
- 28 per cent of businesses paid a ransom globally in Q1 of 2024 according to data collected by Coveware, down from roughly 37 per cent of businesses in 2023.[52]

The above surveys broadly did not use a probability sampling methodology, which limits the ability to generalise inferences to the whole population. It is therefore challenging to quantify the rate of underreporting, the number of entities impacted by ransomware or cyber extortion and the proportion of entities which pay ransoms when impacted with statistical accuracy.

Underreporting of ransomware and cyber extortion limits government's understanding of the cyber threat landscape, such as a lack of accurate quantification of impact on Australian entities and identifying data of ransomware and cyber extortion threat actors. This impedes the ability of law enforcement and other government agencies to protect essential services, Australian businesses and the community and may restrict law enforcement efforts to investigate and prosecute unlawful cyber behaviour.

[46] Sophos State of Ransomware Report 2023, p 24.
[47] Tara Seals, *REvil Gang Promises a Big Video-Game Hit; Maze Gang Shuts Down*, Threatpost, 29 October 2020 <https://threatpost.com/revil-video-game-hit-revenue/160743>.
[48] Ransomware.org Report 2024, p 6.
[49] Delinea, *State of Ransomware 2024 Whitepaper*, 2024, p 3 <https://delinea.com/hubfs/Delinea/whitepapers/delinea-whitepaper-state-of-ransomware-2024-report.pdf> ('Delinea State of Ransomware Report 2024').
[50] SpyCloud, *Spycloud Ransomware Defence Report 2023*, 2023, p 11 <https://engage.spycloud.com/rs/713-WIP-737/images/spycloud-report-2023-ransomware-defense-report.pdf>.
[51] DeepInstinct, *Generative AI and Cybersecurity: Bright Future or Business Battleground?*, 2023, p 11-12 <https://www.deepinstinct.com/pdf/voice-of-secops-4th-edition?hsCtaTracking=982e81ff-d1a0-47a4-9adf-6e279398d361%7C1d16a471-1022-4dff-8d07-dd79dac66a52>.
[52] Coveware Blog.

Why Government intervention is required

The Australian Government requires better quality data and reporting on ransomware and cyber extortion incidents experienced by Australian businesses, to better inform its response to this economic and security challenge. A lack of accurate information undermines the ability of government authorities to assist with consequence management for impacted entities. For example, without comprehensive threat picture information, government authorities are unable to forewarn parties of vulnerabilities or mitigation strategies. This means that products designed to assist businesses uplift their resilience to ransomware and cyber extortion are weaker, which may affect the credibility of Government. Ultimately, this compromises Australia's collective security, inflicts ongoing economic damage and leaves individuals and businesses vulnerable to damaging future cyber incidents.

This requires an increase in the reporting rate for incidents, the timeliness of the reporting and the quality and consistency of the data reported. Improved data reporting would allow for more accurate analysis of the cyber threat landscape for evidence-based decision making and to inform policy decisions. Improved understanding of these threats and the ransomware business model will also drive government and law enforcement agencies' ability to adapt to the rapidly evolving cyber security landscape. This will facilitate rapid and more effective responses to both existing and emerging cyber extortion threats through law enforcement actions, risk mitigation and threat prevention.

Reporting will encourage entities to involve Government in the incident response process. In a 2023 survey, IBM found that when law enforcement was involved in the incident response process, the mean cost impact for the company in responding to the incident (not including any ransom payments) was reduced by 9.6 per cent. Additionally, the total time to identify and contain a cyber incident was 33 days shorter with Government involvement.[53] Entities will continue to be encouraged to voluntarily report and engage with ASD at the earliest opportunity. Timeliness is an important factor when managing a cyber security incident, including ransomware and cyber extortion attacks. As soon as a potential incident is detected, even if it is a false alarm, it should be reported to ASD's ACSC. However, the data collected through a mandatory reporting obligation would allow Government to better support business and other entities to assess and manage the risk of ransomware and cyber extortion through the development of additional targeted guidance material. Sharing of actionable, de-identified threat information by Government to industry will assist in raising awareness of the ransomware threat throughout the economy. The benefits of increased reporting will flow through to industry and the wider community as businesses and the community harnesses this information to enhance awareness, threat horizon scanning, and preventative measures to uplift cyber security preparedness and responsiveness. Whilst industry initiatives such as exploit or vulnerability databases and other cyber security products do exist, Government is uniquely placed to build a comprehensive threat picture and provide advisories and support to businesses. This will be especially valuable for small and medium enterprises that may not otherwise be able to afford complex enterprise cyber security solutions.

In consultation on the proposal, several entities reported that the risk of regulatory action was a substantial disincentive for reporting. A regulatory approach that mandates reporting on a no fault, no liability basis is expected to significantly increase reporting rates. It is thus necessary for the Australian Government to intervene to meet the policy objective of improving data quality about ransomware and cyber extortion.

As part of a broader suite of policy measures under the 2023-2030 Australian Cyber Security Strategy, the Government intends to introduce new cyber security legislation. This can address gaps in Australia's current legislative and regulatory framework to provide the right level of protection to Australian citizens and businesses, which would build cyber risk mitigations for businesses and the community. Mandatory reporting requirements for ransomware and cyber extortion form an important part of the broader strategy, and can ensure that ensure government agencies have sufficient data to inform its response to the ransomware threat. In addition, the new cyber security legislation seeks to:

[53] IBM Data Breach Report 2023, p 6.

- create a regulatory scheme to mandate cyber security standards for smart devices
- establish an obligation limiting how information voluntarily disclosed to ASD and the National Cyber Security Coordinator (NCSC) and persons assisting them during a cyber incident can be shared with, and used by, regulatory agencies
- establish a Cyber Incident Review Board (CIRB) with limited information gathering powers, to conduct no-fault reviews of significant cyber security incidents.

This document does not seek to assess the impact of any of these additional measures. This document only assesses the impact of the mandatory reporting requirements for ransomware and cyber extortion.

The success of this solution will be measured by:

- a significant increase in the volume and scope of data reported to Government
- the development of a detailed ransomware and cyber extortion threat picture
- the development of anonymised and actionable threat reports, as well as clear guidance materials, that can be used by industry to prepare for the threat of ransomware and cyber extortion
- an increase in businesses receiving assistance from government as a result of increased reporting of the impacts of ransomware and cyber extortion.
- a better prepared Australian economy that sees a reduction in the quantity and severity of ransomware impacts over the long term due to increased resilience which disrupts the ransomware business model.

What policy options are being considered?

Option 1: Maintain the status quo – most ransomware reporting remains inconsistent and fragmented

The first option maintains the status quo. This would mean the Government continues to rely on current reporting levels identified above to respond to ransomware and cyber extortion threats. As cybercrime often goes unreported, data and threat information is limited and inconsistent, with each entity reporting different levels of information, which can diminish its usefulness. For example, where some entities may provide extensive and technical information to ASD, other entities may only provide the fact that an incident has occurred without any descriptive information at all. There is no timeframe for reporting, meaning some incidents can be reported weeks or months after they have occurred.

The Government will continue to issue threat advisories and support entities as well as possible. However, the effectiveness of assistance rendered by government is commensurate with the quality of the information it receives.

Case study: ransomware reporting under the status quo

Chandni is a managing director of a successful retail business with outlets across Australia. Her business affected by a crippling ransomware and cyber extortion incident that forces the business to temporarily close. When computers connected to her business' network boot, they display the warning:

ALL YOUR IMPORTANT FILES ARE ENCRYPTED!

The screen displays a link to download a secure browser, an encrypted messaging system with chatroom ID, a bitcoin wallet ID and the quantity of bitcoin requested. Chandni makes the decision to hire a cyber recovery firm to contain the incident and restore her essential systems from backups. She decides to pay the ransom and an automated decryption key is provided. Several days later, she receives an email demanding that she pay another ransom, or sensitive files exfiltrated from her severs would be released for sale on the dark web. She refuses to pay the second ransom and her files are subsequently released for sale.

Several weeks later at a business conference, she attends a presentation on cyber security that lists reporting instructions for reporting voluntary cyber security incidents to ASD's ACSC and explains how they can provide assistance. She decides to report the cyber incident to the *ReportCyber portal*, including a general description of the incident and the name of the group, but not any technical information, the amount of bitcoin requested or the bitcoin wallet ID. She does not advise that she paid a ransom.

Option 2: Encourage voluntary reporting of ransomware demands and payments

The second option focuses on providing additional government resources to improve voluntary reporting of ransomware demands and payments across the whole economy. This option does not require legislation.

Greater engagement with industry would be undertaken through existing mechanisms, such as ASD's Cyber Security Partnerships Programs,[54] the Trusted Information Sharing Network sector groups,[55] media and

[54] Australian Cyber Security Centre, *Australian Signals Directorate's Cyber Security Partnership Program,* Australian Signals Directorate, 2023 <https://www.cyber.gov.au/partnershipprogram>.
[55] Cyber and Infrastructure Security Group, *Trusted Information Sharing Network*, Department of Home Affairs, 2023 <https://www.cisc.gov.au/how-we-support-industry/partnership-and-collaboration/trusted-information-sharing-network>.

social media engagement and publications by the Cyber and Infrastructure Security Group, engagements by the National Office of Cyber Security,[56] noting that industry engagement would continue to be on a voluntary basis. Entities would be encouraged to report ransomware demands and payments that relate to cyber security incidents to the *ReportCyber* portal.[57]

Under this option, all entities would be encouraged to report to the ReportCyber portal when they have experienced a ransomware incident. As part of reporting, entities would be advised to provide the following information:

- information about the reporting entity (ABN, type of entity, whether they are a small/medium/large business, whether they oversee critical infrastructure)
- when the incident occurred and when it was discovered
- what assets and data were affected by the incident
- what quantum of payment has been demanded by the ransomware actor or cybercriminal, what method of payment has been demanded, and any pre-payment negotiations undertaken (if relevant)
- whether the entity made a ransomware payment, and if so quantum of payment, method of payment
- information about the ransomware or cyber-extortion actor
- any communications exchanged in relation to the ransom, and
- any other information relevant to the incident.

The entity can make a report any time during or after an incident and incident response is occurring. Information voluntarily reported to ASD or the NCSC may also be subject to safeguards under the proposed limited use regime.

Case study: ransomware reporting under an enhanced voluntary scheme

Leia is the owner of a medium service business which keeps customers' personal and banking information on its systems. The business is subject to a ransomware attack in which the patient data is stolen and payment of $50,000 to be transferred to a given bank account is demanded via email to recover this information.

Leia has all the information backed up so does not pay the ransom and undergoes the businesses incident response plan. Leia has seen advisory material developed and distributed by the Department of Home Affairs on its social media channels and on the Cyber and Infrastructure Security Centre website, a call for reporting of all ransomware and cyber extortion demands and payments. She decides to report the incident on the *ReportCyber* portal. She enters the following details:

- The name of her business, address, contact details, ABN and the fact that it is a medium business that provides a service
- The time the email demanding ransom was discovered, when it was sent, and the time of the data breach as estimated by Leia
- What data was affected by the incident – how many customers' data had been stolen, details of the personal and financial data that the company stored
- The fact that $50,000 was demanded, that there had been no negotiations between Leia and the threat actor, that the criminal had provided a bank account for transfer of the funds, and the bank account details
- The fact that Leia did not make any payments
- The fact that Leia had been contacted by email and the email address that the demand was sent from

[56] Department of Home Affairs, *Cyber Coordinator*, 26 February 2024 <https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/cyber-coordinator>.
[57] Australian Cyber Security Centre, *Report*, Australian Signals Directorate, 2024 <https://www.cyber.gov.au/report-and-recover/report>.

As Leia does not employ anyone who can investigate this threat actor further, Leia only provides what she knows from the initial incident. This report goes to the Department of Home Affairs which uses this reporting information in tandem with all other reports received to gain a better understanding of the threat environment. This includes information gathering on specific threat actors, on methods being used for ransomware attacks, of the type of businesses targeted, and of any other trends that could help the government develop policies to better protect against future attacks on businesses.

Option 3: Legislate mandatory reporting of only ransomware payments

The third option creates an obligation for captured entities to report ransom payments only, with voluntary reporting (and reporting through other legislated schemes) to continue when a cyber incident occurs and/or a demand is made. This would be supplemented by a no-fault, no-liability principle for entities making a report to ensure that the report would not be used in regulatory action. This reporting obligation would not preclude any information gathered by regulators or law enforcement by other methods in accordance with their existing legislated functions, or directly reported to them, from being used.

There are currently a variety of reporting arrangements for cyber incidents, including under the *Security of Critical Infrastructure Act 2018* and the Office of the Australian Information Commissioner's Notifiable Data Breach scheme, which may inadvertently capture information relating to ransomware and cyber extortion. However, there are currently no reporting obligations that include provision of information relating to the payment of a ransom. Introducing a reporting obligation that could capture this data would address one of the most significant information gaps currently faced by Government agencies in building a picture of the ransomware threat and how Australian entities are being impacted by it.

At the same time, it addresses industry concern of regulatory and law enforcement action by providing assurance through no-fault, no-liability reporting and minimises regulatory burden by avoiding duplication with other analogous cyber incident reporting schemes.

This option would mandate an entity providing information about the ransomware payment to ASD's ACSC within 72 hours of the payment being made. While ASD is not a regulator, ASD's ACSC's reporting portal is already used for mandatory cyber incident reporting under the *Security of Critical Infrastructure Act 2018.* There will be a standardised form that is contemplated to include the following non-exhaustive measures.

- company details (ABN, address, etc.)
- when the incident occurred and when the entity became aware of the incident
- what variant of ransomware was used (if relevant)
- what vulnerabilities in the entity's system were exploited by the attack (if known)
- what assets and data were affected by the incident, what quantum of payment has been demanded by the ransomware actor or cybercriminal, what method of payment has been demanded and any pre-payment negotiations undertaken (if relevant)
- what quantum of payment has been made and what method of payment was used
- the nature and timing of any communications (for example, email), and
- the impact on the reporting entity's infrastructure and customers and anything else relevant.

Entities would also be able to provide additional details to the report on a voluntary basis and will not be penalised for making incomplete reports in good faith, noting that they may still be in the response stage of a cyber-incident.

As this reporting obligation is mandatory, entities found to be non-compliant would face a civil penalty of 50 penalty units.

Case study: mandatory reporting of only ransomware payments

Enzo runs a small software as a service (SaaS) company in Melbourne that focuses on providing artificial intelligence (AI) solutions to cyber tech firms around Australia and overseas. Recently, the business expanded to Sydney and Brisbane. With a small team of his employees, Enzo configured the new admin systems for the businesses in the other locations that could also connect along the same server back to Melbourne, including allowing for a Remote Desktop Protocol (RDP) so his employees could work from home. However, unbeknownst to Enzo, a zero day exploit in the RDP was utilised by a ransomware threat actor to infiltrate his company's systems, where critical business files were locked and encrypted.

A countdown timer for 24 hours appeared in a small window on his desktop, demanding payment of 3 bitcoin be sent to an address.

As Enzo's systems were newly set up, he did not have a backup of the critical files on his computer and as such, his business operations in Melbourne, Sydney and Brisbane have been severely impacted. This includes being unable to pay his employees. Enzo elects to purchase the bitcoin and send his bitcoin wallet ID to the address specified in the demand. Enzo waits patiently as the timer continues to count down, but his files have still not been unlocked, despite making the ransomware payment.

Through his work in the cyber sector, Enzo participated in Town Halls on the new Cyber Security Act and is aware that he has to make a report through ASD's ACSC's *ReportCyber* portal, where he provides the mandatory reporting details, including the name of his company, when the incident occurred, what quantum of payment was demanded and what quantum he paid. He lists how his business has been crippled as it can no longer provide AI solutions to big cyber tech companies in Australia, and overseas.

The information is collated with other similar reports and ASD's ACSC is able to identify a trend that reveals a new ransomware actor is targeting managed service providers of major tech firms internationally. ASD's ACSC is able to develop and distribute threat information to assist these firms prevent future attacks by patching the exploit. De-identified information was distributed to the Australian Federal Police and used to identify the threat actors and initiate a response to disrupt the ransomware threat actor's business model.

This option would be supported by a proportionate civil penalty scheme that would encourage engagement with Government in the first instance. In the event of non-compliance, an entity would be sent a reminder or formal letter in first instance, with civil fines issued for persistent non-compliance with the request to report. The proposed civil penalty is 50 penalty units, where this is necessary. This seeks to strike a balance between an enforceable regime that seeks to avoid punishing companies subject to a ransomware or cyber extortion incident.

Option 4: Legislate mandatory reporting of both ransomware demands and payments

Option 4 contemplates introduction of legislation to require entities to report both:

- when they are impacted by a ransomware attack and receive a demand of payment to decrypt their data or receives an extortion demand not to share ex-filtrated data, and
- if they make a ransomware or extortion payment.

For some entities, this may mean they will be required to report to government twice (once on being impacted and again if a payment is made).

Option 4 includes the same requirements for mandated information as Option 3, however the information would be provided in two separate reports in the event a payment is made. The proposed reporting requirements will mobilise immediate and time-sensitive ransomware and extortion reporting to, provide advice to industry, and build Australia's understanding of cyber extortion trends and the ransomware business model. This would require entities to report within 72 hours of an incident occurring. If a ransom payment were made, entities would also then be required to submit a second report with relevant details. As with Option 3, this option would include protections for industry to avoid reports being used for regulatory or

civil litigation.

Entities would be required to report a cyber incident within 72 hours of the incident being discovered. Reports can be written or oral (to be followed up later with a written report in the correct format). Information to be reported would include such details that, at the time of making the report, the reporting business entity would know or would be able, by reasonable search or enquiry, to find out:

- their Company details (ABN, address etc.)
- when the incident occurred, and when the entity became aware of the incident
- what variant of ransomware was used (if relevant)
- what vulnerabilities in the entity's system were exploited by the attack (if known)
- what assets and data were affected by the incident
- what quantum of payment has been demanded by the ransomware actor or cybercriminal, what method of payment has been demanded, and any pre-payment negotiations undertaken (if relevant)
- the nature and timing of any communications between the entity and the ransomware actor or cybercriminal
- the impact of the incident, including impacts on the entity's infrastructure and customers, and
- any other relevant information about the incident or actor that could assist law enforcement and intelligence agencies with mitigating the impact of the incident and preventing future incidents.

If the entity has made a ransomware payment, they will also be required to provide what quantum of payment has been made and what method of payment was used.

This option would be supported by an almost identical civil penalty regime as option 3, with the only difference being that it would be used to ensure compliance with both ransomware and cyber extortion incidents and payments.

Options for reporting thresholds

In implementing Option 3 or 4 outlined above, the Government is considering two options to ensure the obligation captures a sufficient amount of entities to enhance visibility of the cyber threat, without significantly increasing regulatory burden of businesses recovering from a cyber incident. Setting a larger scope will allow government to learn more about the threat landscape, but this comes at a cost of additional regulatory and administrative burden for businesses.

Option A: Annual turnover of $10 million or greater

While there is no uniform definition of a small or medium sized business across Australian legislation, both the *Income Tax Assessment Act 1997* and the *Competition and Consumer Act 2010* define a small business as one with an aggregate annual turnover of less than $10 million.[58] The *Privacy Act 1988* defines a small business as one with an annual turnover of less than $3 million. To avoid ambiguity, we refer to large businesses as those with an annual turnover of greater than $10 million, medium businesses with an annual turnover of $3 million or greater but less than $10 million, and small businesses with an annual turnover of less than $3 million.

This option captures only large businesses and ensures that this new regulatory requirement would not apply to small or medium sized businesses, which make up approximately 98 per cent of registered businesses in Australia.[59] As small businesses have significantly less resources and may not be able to readily absorb the cost of any reporting burden, this threshold will ensure that the regulatory impost on industry is minimal.

The number of businesses with annual turnover of greater than $10 million per year accounts for around 1.84 per cent of total registered businesses. However, this metric does not necessarily represent the percentage of the Australian economy captured. Larger businesses tend to employ more people, create more economic

[58] *Income Tax Assessment Act 1997* s 328-110; *Competition and Consumer Act 2010*, sch 1, s 23(4).
[59] Australian Bureau of Statistics, *Counts of Australian Businesses including Entries and Exits*, 22 August 2023, Data Cube 1, Table 17 <https://www.abs.gov.au/statistics/economy/business-indicators/counts-australian-businesses-including-entries-and-exits/latest-release> ('ABS Counts of Australian Businesses 2019-23').

value and serve a greater number of customers. For example, if a ransomware incident impacted a major supermarket that served 30% of the Australian population, the impact of that ransomware incident would be greater than if a single small business was impacted. The aggregate coverage of the Australian economy by capturing businesses with an annual turnover of greater than $10 million is significantly greater than 1.84 per cent.

Additionally, critical infrastructure entities are proposed to be subject to the ransomware requirements regardless as to the monetary threshold applied. Protecting Critical Infrastructure and Systems of National Significance regulatory reforms (CISoNS) Regulation Impact Statement (RIS) calculated that there were approximately 340 small businesses and 850 medium businesses that otherwise may not be captured by the threshold, bringing the total to 48,908 businesses.

While this threshold does capture a significant proportion of the economy, the majority of submissions to the Consultation Paper that commented on the ransomware reporting measure (~60 per cent) supported a lower threshold than $10 million.[60] Key reasons put forward in the submissions include the need for a more comprehensive picture of the ransomware threat, the possibility of creating a counter-intentional incentive for criminals to target small businesses.

Option B: Annual turnover of $3 million or greater

Stakeholder feedback to the Consultation Paper noted reasonable support (~17 per cent) for a reporting threshold under $2 million. Stakeholders also noted strong support for a threshold aligned with existing requirements around cyber incident reporting in the *Privacy Act 1988* (~20 per cent).[61] In total, the majority of stakeholders sought a threshold less than $10 million (~60 per cent).

In response to this feedback, the Government recommends a threshold of $3 million. While the Government has provided in principle support for the recommendation from the Privacy Act Review to remove this threshold, aligning with a current obligation that is familiar to small and medium sized entities will ensure consistency across incident reporting obligations without introducing regulatory burden to businesses not currently subject to reporting obligations.

Based on comparative ABS data, the total number of businesses with an annual turnover of $3 million or greater is approximately 170,009 or 6.56 per cent of total businesses.

Noting critical infrastructure entities are proposed to be subject to the ransomware requirements regardless as to the monetary threshold applied. The CISoNS RIS notes approximately 340 small businesses that may not be captured by the $3 million threshold, bringing the total to 170,349 businesses.

Estimation of businesses with annual turnover of $3 million or greater

The ABS report the number of businesses with an annual turnover of at least $2 million and less than $5 million.

Given the ABS report 117,843 businesses in the $2 million to less than $5 million threshold[62], where X is less than $5 million, Y is $2 million and Z is the new threshold of $3 million:

$$Total\ Businesses_{X-Z} = \frac{Threshold(X) - Threshold(Z)}{Threshold(X) - Threshold(Y)} \times Total\ Businesses_{X-Y}$$

$$Total\ Businesses_{\$3m-<\$5m} = \frac{4{,}999{,}999.99 - 3{,}000{,}000}{4{,}999{,}999.99 - 2{,}000{,}000} \times 117{,}843$$

$$Total\ Businesses_{\$3m-<\$5m} = 78{,}562$$

$$\therefore Total\ Businesses_{\$3m+} = 78{,}562 + 43{,}729 + 47{,}718 + 340 = 170{,}349$$

In the absence of additional data or a better fitting model, this calculation assumes that there is a uniform distribution of businesses within the threshold.

[60] This is compared to only 20% of submissions that responded to the ransomware measure supporting a $10 million or higher threshold, and 20% seeking a non-monetary or alternative threshold.
[61] *Privacy Act 1988* s 6D(1), s 6 (definition of 'APP entity'), 6C, 26WE.
[62] ABS Counts of Australian Businesses 2019-23.

What is the likely net benefit of each option?

Approach to determining costs

Costs will be estimated by the marginal impact of the proposed options that would be borne by entities that meet the relevant thresholds. Costs per business are likely to be too small to meaningfully pass on through cost increases for goods and services. Community organisations and individuals are not likely to be directly affected.

Initial costs for captured entities

All entities captured by the relevant thresholds would have initial administrative costs. This would involve one member per entity to dedicate approximately 3 hours and 15 minutes of their time to become aware and disseminate information of their new obligations to report a ransomware payment to the relevant Commonwealth entity.

This would include:

- one hour for an individual to read guidance documents that will be provided by the Department of Home Affairs on an entity's obligations
- an estimated two hours dedicated to creating standard operating procedure or equivalent documentation for the organisation to adhere to their obligations,
- a final 15 minutes for an individual to disseminate the information throughout their organisation.

The initial administrative cost for all entities is calculated as $276.80 per entity.[63] These figures are calculated in the same manner as the Mandatory Cyber Incident Reporting obligation in the CISoNS RIS, but with updated values for the 2023-2024 financial year.[64]

It should be noted that for an entity with an annual turnover of $3 million – the lowest contemplated threshold in the presented options – the initial cost would account for less than 0.001 per cent of the organisation's turnover, representing a negligible impact on the individual entities. Thus, while the economy-wide impacts in total appear substantial, there will be no significant impact on any individual entities.

Ongoing cost during a cyber incident

In 2020-2021, ASD reported that there were roughly 500 ransomware reports, which was an increase of nearly 15 per cent from the previous year.[65] However, in 2021-22 ASD reported that there were 447 ransomware reports.[66] ASD did not report the number of ransomware incidents in 2022-2023.

Using these values of voluntary ransomware reports, and based on private surveys that estimate under-reporting in question one, we estimate that there will be approximately three times the number of ransomware and cyber extortion incidents, which is approximately 1451 incidents.

---

[63] In line with the introduction of mandatory cyber incident reporting requirements for critical infrastructure in the *Security of Critical Infrastructure Act 2018*, no legal expertise is expected to be required to understand the obligations to report or to report for ransomware demands or payments. See Department of Home Affairs, Protecting Critical Infrastructure and Systems of National Significance regulatory reforms Regulation Impact Statement <https://oia.pmc.gov.au/sites/default/files/posts/2020/12/ci_sons_regulation_impact_statement_-_final_second_pass.pdf > ('CISoNS RIS').

[64] For labour costs, the scaled up rate of $85.17 per hour was used to reflect OIA guidance. See, Office of Impact Analysis, *Regulatory Burden Measurement Framework*, Department of the Prime Minister and Cabinet, 2022, p 12 <https://oia.pmc.gov.au/sites/default/files/2024-02/regulatory-burden-measurement-framework.pdf>.

[64] CISoNS RIS.

[65] Australian Cyber Security Centre, *July 2020 to June 2021 Annual Cyber Threat Report*, Australian Signals Directorate, 2023 p 10 <https://www.cyber.gov.au/sites/default/files/2023-03/ACSC%20Annual%20Cyber%20Threat%20Report%20-%202020-2021.pdf>.

[66] Australian Cyber Security Centre, *July 2021 to June 2022 Annual Cyber Threat Report*, Australian Signals Directorate, 2022, p 47 <https://www.cyber.gov.au/sites/default/files/2023-03/ACSC-Annual-Cyber-Threat-Report-2022_0.pdf>.

Additionally, private surveys in question one estimated between 20 per cent and 75 per cent of Australian businesses would opt to pay a ransom. Surveys with larger samples tended towards the lower end of the scale. Therefore, we estimate that approximately a third of businesses would pay a ransom. Based on the above estimate of total ransomware and cyber extortion incidents, we estimate that approximately 484 of these proceeded to payment of the extortion demand.

While all businesses are targeted by ransomware cyber extortion, cybercriminals are incentivised to target larger entities as part of 'big game' ransomware campaigns, as larger entities can provide a larger payout.[67] Indeed, in a survey of Australian Companies, McGrath Nicol found that companies with 1000 or more employees were twice as likely to suffer from multiple ransomware attacks as a smaller entity.[68] One US survey of 300 entities found ransomware targeted 65 per cent of mid-sized entities (employees 51-499) and 22 per cent of large entities (employees 500+).[69] This is broadly consistent with the 2023 Microsoft Digital Defence Report, which found 30 per cent of all attacks target entities with more than 500 employees.[70]

We estimate that due to big game hunting, large businesses may comprise 30 per cent of total reports, medium businesses may comprise 20 per cent of reports and small businesses would comprise the remaining 50 per cent of reports. Applying this total to the percentage of large and medium businesses that may make ransomware payments, it is estimated large businesses may make 435 reports and medium businesses may make 290 reports, for a total of 726 reports across both categories.[71]

After a ransom payment is made, it is estimated a report would require 3 hours of an individual employee's time.

This would involve:

- a member of an organisation becoming aware of a ransomware payment being made and consulting relevant standard operating procedures to determine reporting requirements (15-30 minutes);
- consulting internally to gather the relevant information from the incident, such as the payee (cryptocurrency wallets and addresses, relevant correspondence), the quantum of payment and the method of payment (30-90 minutes); and
- summarising the incident in an email, through a phone call or in a web form to the relevant Commonwealth entity (15-30 minutes).

This leads the individual reporting costs to be uniform across entities at a cost of approximately $255.51 per incident based on up to 3 hours of labour. This is with the caveat that reporting time may differ among entities, due to differences in an entity's efficiencies in collecting information and reporting cyber incidents to a regulator. Similarly, the first time an entity complies with the reporting obligation may take three hours, but as efficiencies develop in the compliance process within an entity, the second time an entity needs to report a payment, the process may be more efficient and cost less in labour hours.

Approach to determining benefit

Benefits will be estimated on the ability of the option to enhance the Government's collection of ransomware and cyber extortion demands and payments, through ASD, to inform efforts to disrupt and break the ransomware business model. These capabilities may include the targeted intrusion into foreign networks, blocking access to stolen or sold data and removing terrorist propaganda from websites and chatrooms. These reports will contribute to the national ransomware threat picture and allow the Government to see what threat actors are active, how they compromise or infiltrate networks, what quantum and method of

---

[67] Malwarebytes, *Key Learnings from "Big Game" Ransomware Campaigns*, 2023 October 26 <https://www.malwarebytes.com/blog/news/2023/07/ransomware-making-big-money-through-big-game-hunting>; Malwarebytes State of Malware Report 2024, pp 6-9; CrowdStrike, *2024 Global Threat Report*, 2024 <https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf>; Department of Home Affairs, *Ransomware Action Plan 2021*, October 2021 <https://www.homeaffairs.gov.au/cyber-security-subsite/files/ransomware-action-plan.pdf>.

[68] McGrath Nicol, *Ransomware: A Cost of Doing Business?*, 2023 <https://a.storyblok.com/f/186891/x/4a4edc8426/mcgrathnicol_flyer-ransomware-survey-2023_v14.pdf>.

[69] Delinea State of Ransomware Report 2024, p 3.

[70] Microsoft Threat Intelligence, *Microsoft Digital Defense Report*, Microsoft, October 2023, p 18 <https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023>.

[71] This assumes 20% reports are made by large businesses, and 30% by medium businesses, 50% small business. This is based on stakeholder feedback that small and medium businesses remain significant targets for ransom. This also assumes that that despite the relatively smaller portion of businesses that are large businesses, they are disproportionately targeted through 'big game ransomware campaigns' as more lucrative targets. While there are conflicting views on the proportion of incidents that affect big business, this Impact Analysis assumes a larger proportion so as not to underestimate the impact on business.

payment they demand, which may in turn benefit law enforcement operations and investigations.

Through the building of the national ransomware threat picture and identifying ransomware and cyber extortion trends, the Government will be able to provide more tailored advice to industry and business on how to better protect their networks, uplift their cyber hygiene and remedy common vulnerabilities into their networks. These benefits will also be passed onto the consumers of industry products and services.

An assessment of these benefits will be qualitative in nature, as the assessment of how industry and business interpret or use tailored Government advice is not quantitative.

Option 1: Maintain the status quo – most ransomware reporting remains inconsistent and fragmented

Cost

Without an increase in the quantity and scope of ransomware and cyber extortion data, the Government and law enforcement agencies would not be able to improve their response to ransomware and cyber extortion incidents, commensurate with the growing threat. Additionally, Australia will not benefit from improvement in preparedness to deter cyber criminals and ultimately fail to see a strengthening of our collective cyber resilience.

Option 1 presents the most significant cost of ongoing gaps in awareness of the threat of ransomware. As described above, ransomware has been described by ASD as remaining the most destructive cybercrime threat in 2022-23 to Australian entities.[72] However, there is evidence that ransomware demands and payments are significantly underreported. Maintaining the status quo will not remedy that gap, limiting the advice that Government can provide to industry and the response of law enforcement to effectively address the threat of ransomware. Without the information required to assess effective policy and operational solutions, Government will be unable to respond effectively. This in turn will limit the impact of Government policies from stemming the severe economic impact associated with ransomware.

Benefit

Industry will face no additional regulatory costs, but neither will they receive tangible benefits under the status quo.

Net benefit

Option 1 is not capable of addressing gaps in awareness of the ransomware threat picture. The status quo will not enable the enhancement of data collection on ransomware and cyber extortion necessary to break the ransomware and cyber extortion business model. The absence of this data is already keenly felt. Further, the lack of aggregate data means that Government cannot develop comprehensive intelligence products and threat assessments that would otherwise directly bolster the cyber security of potential victims and contribute to the breaking of the ransomware and cyber extortion business model.

Option 2: Encourage voluntary reporting of ransomware demands and payments

Cost

Even with additional government resources to encourage voluntary reporting, the option will have limited effectiveness. Benefits associated with the additional resources will be restricted as it will be at the discretion of industry to inform the Government of ransomware reports and payments, and fail to resolve industry concerns about the risks of reporting to Government. In the absence of clear legislated requirements for the type and quantity of information required, reports from industry are also unlikely to contain the information required in sufficient detail.

Option 2 will only impose voluntary costs on industry, as it would be up to businesses as to whether reporting was in their best interests. Likewise costs associated with existing cybersecurity incident reporting regimes in different sectors would continue to carry costs for industry, but these are outside of the scope of this Impact

[72] ACSC Cyber Threat Report 2022-23, p 48.

Analysis, as they would have been the subject to separate analysis prior to their introduction.

For entities that elect not to voluntarily report ransomware demands or payments, there are no regulatory costs. However, we estimate the costs to the business to make a voluntary report in the same manner as Options 3 and 4. This is because such entities will continue to operate under the status quo regulatory environment. However, where a business elects to voluntarily report, the costs will be similar per business to those calculated in either Option 3 or 4, depending on the type of report and level of detail that the affected entity elects to provide.

All relevant minor costs to Government to implement engagement and awareness raising activities would be absorbed under existing programs and capacity.

Total costs

Table 1. Marginal costs to businesses for voluntary reporting under option 2

Cost description	Voluntary reporting
Total number of entities	56,783
Aggregated administrative cost (single year)	$15,717,676.35
Number of ransomware payments (est.)	202
Number of ransomware demands (est.)	605
Total number of reports (payments + demands)	806
Aggregated reporting cost (single year)	$206,011.99
Aggregated reporting cost (10 years)	$2,060,119.86
Total aggregated costs to industry (10 years)	$17,777,796.20

Benefit

Option 2 will provide some improvement to the ransomware threat picture available to Government should entities engage with the voluntary reporting regime, even though the number of reports made is expected to be less than if reporting was mandatory. An enhanced threat picture informed by these reports would have a beneficial impact on the Government's evidence-based decision making, and would further inform the tailored advice given to industry and business. This tailored advice would assist industry and business in uplifting their overall cyber hygiene and help them remedy common vulnerabilities into their networks, to make them harder targets.

Should entities engage with the voluntary reporting regime, the Government intends to collate and distribute the information received providing anonymised detail to assist entities to prepare for, respond to and bounce back from a ransomware or cyber extortion incident. This will be beneficial in helping entities to be aware of current threats, attack methods, and vulnerabilities that are being exploited, so that they can invest in more targeted cyber incident prevention methods.

The Government would also benefit from this voluntary reporting, should entities choose to engage with it, and will provide enhanced visibility about what ransomware threat actors are active, how they compromise or infiltrate networks, what quantum and method of payment they demand, which may in turn benefit law enforcement operations and investigations.

Net benefit

Option 2 is not expected to have a sufficient positive impact in addressing gaps in awareness of the ransomware threat picture. The option does not substantially change the current reporting environment which already includes public communications efforts to promote voluntary reporting. Amplifying public

communications is likely to have some positive impact, but this will not ensure sufficient data concerning the ransomware threat is gathered across the economy. Additional engagement will increase reporting levels, but is unlikely to increase reporting to the levels as far as can be achieved under alternate options.

Option 3: Legislate mandatory reporting of only ransomware payments

Costs

Costs are calculated as set out in above, and are set out in the table below. Additionally, some of the costs of Option 2 will also apply to this option as some entities will elect to make a voluntary report where they do not fall under the relevant threshold.

Total costs

Table 2. Costing calculations for option 3

Cost description	$3 million+	$10 million+
Total number of entities[73]	170,349	48,908
Aggregated administrative cost (first year only)[74]	$47,153,029.04	$13,537,856.67
Number of ransomware payments (est.)	242	145
Aggregated reporting cost (single year)[75]	$61,804	$37,082.16
Aggregated reporting cost (10 years)[76]	$618,035.96	$741,114.20
Total aggregated costs to industry (10 years)[77]	$47,771,064.99	$13,908,678.24

While the cost to businesses at the $3 million or greater annual turnover threshold appears to be significantly higher, the individual cost per entity is estimated to be uniform across entities. Even for the smallest of affected entities, this cost equates to less than 0.001 per cent of annual turnover. This negligible amount is not expected to materially affect individual entities' overall financial position.

The Australian Government recognises the disproportionate impact that cyber incidents have on small and medium businesses, and the challenge that these businesses face to uplift cyber security without appropriate support and guidance. The Government is committed to minimising regulatory burden where practicable, especially to small and medium businesses. The 2023-2030 Australian Cyber Security Strategy seeks to address these challenges through a range of programs targeted to small and medium businesses.

Benefit

Immediate and time-sensitive ransomware and cyber extortion reporting will provide the Australian Government key information to, facilitate advice to industry, and build Australia's understanding of cyber extortion trends and the ransomware business model. Gaining this information is essential to breaking the ransomware business model, as law enforcement and intelligence agencies can provide tailored support to all businesses in Australia, particularly small business which can be more vulnerable to ransomware and

[73] ABS Statistics report 47,718 businesses with an annual turnover of over $10 million—these were considered "large businesses". The total for large businesses and responsible entities for critical infrastructure not otherwise captured by these statistics is 48,908. Additionally, an approximate of 170,009 businesses have an annual turnover of at least $3 million. The remainder of businesses that fall below the $3 million threshold were considered "small businesses" and are not subject to these calculations. The total, including critical infrastructure entities not otherwise captured by these statistics, is 170,349. See also above calculation call-out box, 'Estimation of businesses with annual turnover of $3 million or greater'. CISoNS RIS; ABS Counts of Australian Businesses 2019-23, table 17.
[74] Calculated by multiplying the number of businesses that will be subject to the reporting requirement by the fixed calculated administrative cost of $276.80.
[75] Calculated by multiplying the number of ransomware payments by the fixed calculated reporting cost of $255.51.
[76] Calculated by multiplying the total single year reporting cost by 10.
[77] Calculated by adding 'Aggregated reporting cost (10 years)' to 'Aggregated administrative cost (first year only)'.

cyber extortion.

Overall, it is likely that the enhancement of data collection on ransomware and cyber extortion incidents will ultimately improve cyber security and privacy protection across the Government, businesses and the community. Through enhanced awareness of the ransomware and cyber extortion threat, government will be able to amplify the provision of timely support to industry to assist law enforcement and intelligence agencies in the disruption of threat actor activities and responding to cybercrime.

The Government intends to collate and distribute the information received quarterly providing anonymised detail to assist entities to prepare for, respond to and bounce back from a ransomware or cyber extortion incident. This will be beneficial in helping entities to be aware of current threats, attack methods, and vulnerabilities that are being exploited, so that they can invest in more targeted cyber incident prevention methods. This option would give industry more information on incidents where a ransom has been paid, but not necessarily on ransomware threats in general.

These actions can help Australia become a hard target for cybercriminals as the government can use information gained from mandatory reports such as what ransomware actors are proliferating, their methods of intrusion, how they contact victims and what they demand. This information can be used to inform the Australian public on how to better protect and secure their data, systems and assets, promote better cyber hygiene practices and avoid common security mistakes that ransomware actors and cybercriminals can exploit. This in turn should reduce the frequency and likelihood of cyber incidents impacting Australian entities and individuals, including loss of reputation, data and finances, thus contributing to the maintenance of overall national prosperity.

According to the Australian Transactions and Analysis Centre (AUSTRAC), many ransomware and cyber extortion victims may be hesitant to report a payment to Government due to fear of compliance action from the Government.[78] A number of submissions echoed this concern.[79] A legislated requirement to report ransomware and cyber extortion payments with a built in no-fault, no-liability mechanism with sufficient clarity will be sufficient to address this concern.

Case study: example of how ransomware payment reporting improves outcomes

Threat actors are increasingly targeting hospitals with ransomware attacks due to the sensitive personal nature of the data that they hold along with the urgency of risk to human life caused by these attacks. This increased risk may result in a higher frequency of these ransoms being paid in order to recover the data or asset access that has been stolen as quickly as possible.

The incident response necessary to be undertaken by the hospital is likely to be extensive, and this along with the additional workload of functioning during an attack means that reporting the incident voluntarily is unlikely to be a priority. However, with mandatory reporting of ransomware payments, the hospital would be obligated to report if they made a payment.

The mandatory reporting thus will give government visibility of the targeting of hospitals by ransomware actors, the techniques most commonly deployed and the high rates of payments that are made by affected hospitals. Government can then consider an appropriate policy response to provide the right sort of assistance to hospitals to increase their cyber resilience to prevent these attacks, as well as assist in their response. This could include guidance and research investment for increased security of software and datasets specific to those used in hospitals. It could also include engaging with the sector to provide assistance in developing appropriate response procedures tailored to hospital and medical systems and businesses to help them recover more effectively, reducing the temptation to pay the ransom.

The government will also use trends provided to them by these reports to investigate and dismantle threat actors. These measures will lead to an overall decrease of ransomware attacks on hospitals as well as decrease ransomware payments made by hospitals when incidents do occur.

---

[78] Australian Transaction Reports and Analysis Centre, *Detecting and Reporting Ransomware - Financial Crime Guide*, April 2022 p 5 <https://www.austrac.gov.au/sites/default/files/2022-04/AUSTRAC_FCG_DetectingAndReportingRansomware_FINAL.pdf>.
[79] ANZ Submission, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, March 2024 <https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/ANZ-submission.PDF> ('ANZ Submission'); The Australian Banking Association *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, March 2024 <https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/Australian-Banking-Association-ABA-submission.PDF> ('ABA Submission').

Net benefit

While this option does have reasonably high initial administrative costs for all entities, the ongoing cost to industry is significantly less than Option 4. While Option 4 does identify a higher benefit, due to increased threat picture coverage, Option 3 balances regulatory impost with ensuring the most critical information is collected: information about ransomware and cyber extortion threats that follow through and cause the most harm to Australian entities. Obtaining ransomware and cyber extortion payment reports, rather than both, reduces duplicative reporting while retaining a significant portion of the intelligence value.

Option 4: Legislate mandatory reporting of both ransomware demands and payments

Costs

This option builds on the regulatory cost calculation from Option 3, using the same set of assumptions, the same cost of labour and the same cost for establishment. The primary difference is the inclusion of costings for reports of the initial demand. It is unlikely that the quantitative regulatory burden experienced by organisations will vary between reporting of ransomware demands and payments, as the same information is required from the affected entity just in relation to different triggers.

As above, it is estimated that there are approximately 1451 ransomware and cyber extortion demands made each year and 484 ransomware and cyber extortion payments based on those demands. The same costs that apply to Option 3 would apply per report, per entity at $255.51. This is irrespective of whether the report is for a demand or a payment as the process will be essentially identical. Additionally, some of the costs of Option 2 will also apply to this option as some entities will elect to make a voluntary report where they do not fall under the relevant threshold.

Table 3. Costing calculations for option 4

Cost description	$3 million+	$10 million+
Total number of entities	170,349	48,908
Aggregated administrative cost (single year)	$47,153,029.04	$13,537,856.67
Number of ransomware payments (est.)	242	145
Number of ransomware demands (est.)	726	435
Total number of reports (payments + demands)	968	581
Aggregated reporting cost (single year)	$247,214.38	$148,328.63
Aggregated reporting cost (10 years)	$2,472,143.83	$1,483,286.30
Total aggregated costs to industry (10 years)	$49,625,172.86	$15,021,142.97

While the implementation costs remain the same between, the yearly cost of reporting is estimated to be roughly three times higher than Option 3.

Furthermore, requiring information reporting for compliance purposes in the early stages of a cybersecurity incident is likely to be significantly more burdensome for an impacted entity than reporting during later stages of an incident, as the entity is actively engaged in managing the immediate crisis associated with a ransomware and cyber extortion incident. During this period, entities are typically stretched and focussing their full resources on the problem, and don't have the capacity to meet reporting demands that are not completely necessary.

Reporting requirements during this early phase of an incident are likely going to be on top of existing reporting requirements under other legislative frameworks, thus exacerbating the burden and introducing

duplication. For example, an entity may be required to report:

- under the *Security of Critical Infrastructure Act 2018* if they are a responsible entity for a critical infrastructure asset specified in the rules.
- eligible data breaches if they are an entity covered by *Privacy Act 1988* if it is likely to result in serious harm to an individual whose personal information is involved.
- under the *Consumer Data Right* if they are Accredited Data Recipients under the Consumer Data Right and experience a data breach.
- under the *My Health Records Act 2012* if they are an entity under the Act and become aware of unauthorized collection, use, or disclosure of health information, or an event occurs that may have compromised the integrity of the My Health Record System.
- Under the Australian Prudential Regulation Authority if they are regulated by APRA experience an incident that could have material effect on the entity or its customers.
- and other relevant reporting regimes.

This burden related to the limitations on available resources during the early stages of an incident response are difficult to quantify financially, but nonetheless are considered.

Benefit

Option 4 proposes measures that collect significantly more information than Option 3, as this option captures demands made as well as when the payment is made. This means the breadth of data is greater, as well as the depth of the data, capturing entities who may be subject to a ransom demand but elect not to make the payment. Collecting information at multiple time points creates a more granular view of the threat of ransomware and cyber extortion to Australian entities.

The Government intends to collate and distribute the information received, providing anonymised detail to assist entities to prepare for, respond to and bounce back from a ransomware or cyber extortion incident. This will be beneficial in helping entities to be aware of current threats, attack methods, and vulnerabilities that are being exploited, so that they can invest in more targeted cyber incident prevention methods. Option 4 would give the most information which can be distributed back out to industry, providing information on both ransomware payments and attacks.

It is expected that there would be more than double the ransomware and cyber extortion demands made per year than the ransomware and cyber extortion payments made per year. These extra reports can provide additional streams of information from entities that are subject to ransom demands, but do not make a payment, can be used to provide a more enhanced threat picture to intelligence and law enforcement agencies, which may support Government policy and operations to break the ransomware business model.

Net Benefit

Option 4 does not provide the best balance of costs and benefits. Compared to the other options considered, this would provide the most comprehensive picture of cyber extortion and ransomware. This option would provide the Government with significantly more reports and a more granular view of the ransomware and cyber extortion threat picture (allowing the Government to have visibility over where ransomware and cyber extortion demands are made, not just payments). As costed in Option 3, the individual uniform cost to industry for reporting payments is less than 0.001% of annual turnover, adding the obligation to report ransomware and cyber extortion demands to Government will cost (separating out from initial setup costs) approximately three times as high. The value of intelligence gained from increased reports given to Government is not proportionate to placing another mandatory reporting obligation on large-to-medium businesses with an annual turnover of $3 million or greater, as there are other extensive reporting requirements for entities experiencing a cyber-incident already.

Importantly, these costs are not distributed evenly amongst entities, rather some entities will face double the reporting costs of Option 3. Whilst it may be determined in the future that the value of those reports outweighs the additional regulatory cost, there is currently no evidence available to support that position.

However, this option may also create duplication with other schemes, and increase the regulatory burden for businesses responding to a cyber incident. As noted in Option 3, there are a variety of other schemes that mandate reporting of cyber incidents to various subsets of Australian entities, each with their particular

requirements. Additionally, there are existing channels for voluntary reporting, such as through ASD's *ReportCyber*.

While a more comprehensive reporting scheme would address gaps in existing legislation, it would be challenging to justify duplication of this reporting. Stakeholder feedback was strongly against duplication of existing reporting requirements and/or requested that existing reporting obligations be used to acquit a new ransomware reporting obligation. While the latter option may be possible over the long term, this would require complex amendments across many acts of legislation. This would preclude enhancing data collection in the short term to inform policy and operational responses to ransomware and cyber extortion that is already having severe impacts on Australian entities.

Consultation and feedback

From 18 December 2023 to 1 March 2024, the Department of Home Affairs consulted industry on the 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation Paper. During this period, the Department held over 50 public town hall and deep dive sessions, roundtables and bilateral meetings with impacted stakeholders and received over 130 written submissions from industry and government stakeholders.

Scope of reporting obligations

What we heard …

Stakeholders support the introduction of limited mandatory obligations, so long as the burden on impacted entities is reasonable, and accounts for overlaps with other mandatory reporting schemes.[80] Stakeholders supported aligning the mandatory ransomware reporting obligation with existing regulatory schemes, ensuring entities are able to acquit the obligation through regulatory reporting if all relevant information is provided. A few submissions requested minimal mandatory information requirements, or that only the fact that a ransomware attack has occurred should be mandatory to report.[81]

There is broad support for reporting information regarding threat vectors, identity and behaviour of attackers, targeted sectors and systems, persistent vulnerabilities, and impacts of attacks.[82] Submissions consistently supported a focus on useful, actionable information which could be used to mitigate risks and build resilience across sectors.

Stakeholders supported aligning the mandatory ransomware and cyber extortion reporting obligation with existing regulatory schemes, ensuring entities are able to acquit the obligation through regulatory reporting if all relevant information is provided.[83] Some submissions requested minimal mandatory information requirements, or that only the fact that a ransomware or cyber extortion incident has occurred should be mandatory to report.[84] Some submissions supported mandatory reporting in cases where a payment is made, but not in other cases.[85] Many suggested encouraging voluntary reporting for all entities and incidents, to maximise information sharing without imposing regulatory burden on entities.[86]

---

[80] See e.g., MDR Security, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, 1 March 2024 <https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/MDR-Security-submission.PDF> ('MDR Security submission'); Customer Owned Banking Australia, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, 2024 <https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/Customer-Owned-Banking-Association-COBA-submission.PDF>; Digital Service Providers Australia and New Zealand, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, 2024 <https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/Digital-Services-Providers-Australia-New-Zealand-DSPANZ-submission.pdf> ('DSPANZ Submission'); ASX, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, 1 March 2024 < https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/ASX-submission.PDF> ('ASX Submission').

[81] MDR Security submission; IoT Alliance, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, 1 March 2024 < https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/IoT-Alliance-submission.PDF> ('IoT Alliance Submission').

[82] Insurance Council of Australia, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, 1 March 2024 < https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/Insurance-Council-of-Australia-ICA-submission.PDF> ('Insurance Council Submission').

[83] Black Ink Legal, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs <https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/Black-Ink-Legal-submission.PDF> ('Black Ink Legal Submission').

[84] MDR Security submission; IoT Alliance Submission.

[85] BSA | The Software Alliance, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, 29 February 2024 <https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/BSA-submission.PDF> ('Software Alliance Submission').

[86] Federation University, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, 29 February 2024 <https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/Federation-University-submission.PDF>, Macquarie University, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, 1 March 2024 <https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/Macquarie-University-and-Threat-Defence-submission.PDF> ('Macquarie University

However, various submissions also noted the provision of extensive information could place significant burden on small businesses, and that requiring comprehensive reporting could discourage early reporting.[87]

How we responded…

In response to stakeholder feedback on the benefit of each of ransomware demand reporting and ransomware payment reporting, and Government feedback on the feasibility of reducing the reporting burden, the Department proposed to introduce a mandatory reporting obligation only in circumstances where a ransom or cyber extortion payment is made (**Option 3**). Reporting for ransomware or cyber extortion demands will be voluntary and encouraged through public outreach.

The Department supported industry's call for minimum mandatory reporting requirements, rather than onerous reporting requirements, and will seek to enable a company to acquit the requirement in a user friendly format. The obligation to report will also be included in the single reporting portal on cyber.gov.au.

To ensure the proposal for no-fault, no-liability reporting is applied in practice, the Department proposes good faith provisions be included, where possible, in law.

Annual turnover threshold to identify affected entities

What we heard …

Key stakeholder concern is a lack of clarity as to the purpose of the obligation, particularly as it relates to reporting of ransomware demands, and how reporting by 1.7 per cent of Australian businesses would meaningfully enhance the threat picture.[88]

The majority of stakeholder responses (approximately 60 per cent), across industry groups, government and business, supported a threshold below the proposed $10 million turnover.[89] A significant number of submissions recommended a lower threshold of $3 million in alignment with the *Privacy Act 1988* small business thresholds,[90] others suggested the threshold be lowered to under a $2 million threshold.[91] There was some support for the proposed $10 million turnover threshold (20 per cent), but only 10 of these had firm or unqualified support for the threshold. [92] For the remainder, their concerns might be ameliorated by selecting Option 3 over Option 4, to minimise the regulatory burden on those businesses.

Cyber security and technology firms largely supported lowering the threshold, arguing that the $10 million

---

Submission'); The Cybersecurity Coalition, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, 29 February 2024 <https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/The-Cybersecurity-Coalition-TCC-submission.PDF> ('Cybersecurity Coalition Submission').

[87] DSPANZ Submission; ASX Submission.

[88] See e.g., Law Council of Australia, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, 15 March 2024 < https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/Law-Council-of-Australia-submission.PDFthin Australia>, Australian Chamber of Commerce and Industry, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, 1 March 2024 <https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/Australian-Chamber-of-Commerce-and-Industry-ACCI-submission.PDFns> ('ACCI Submission'); Council of Small Business Organisations Australia, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, 12 March 2024 <https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/Council-of-Small-Business-Organisations-Australia-COSBOA-submission.PDF> ('COSBOA Submission'). Noting that this was the figure quoted by submissions, it reflects data from the previous ABS reporting period. Current estimates are 1.8%, see ABS Counts of Australian Businesses 2019-23, table 17.

[89] See e.g., Software Alliance Submission; Splunk, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, 1 March 2024 <https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/Splunk-submission.PDF> ('Splunk Submission'); ACCI Submission; ABA Submission; Communications Alliance, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, 1 March 2024 < https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/Communications-Alliance-submission.PDF>.

[90] See e.g., Software Alliance Submission; Amazon Web Services, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, 1 March 2024 https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/Amazon-Web-Service-AWS-submission.PDF>.

[91] Financial Services Council, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, 9 March 2024 < https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/Financial-Service-Council-FSC-submission.PDF>.

[92] See e.g., Australian Industry Group, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, 1 March 2024 < https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/Australian-Industry-Group-Ai-submission.PDF> ('Ai Group Submission'), Sydney Airport, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, 1 March 2024 <https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/Sydney-Airport-submission.PDF>, COSBOA Submission; ACCAN, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, 1 March 2024 < https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/Australian-Communications-Consumer-Action-Network-ACCAN-submission.PDF>.

threshold may not achieve coverage required to build an adequate threat picture.[93]

Some submissions suggested the obligation should not be based on turnover, but instead should be based on entity risks, sector and other considerations.[94] A number suggested all entities should be subject to the obligation,[95] with suggestions that tiered reporting requirements could be applied based on sector, turnover, and sensitivity of the entities information holdings.[96] Stakeholders also suggested that entities subject to other reporting obligations (including under the SOCI Act) should be exempt from the new obligation, or be able to acquit the reporting requirement through other regulatory disclosures.[97]

How we responded…

Reflecting on consistent feedback to capture more entities, and to take account of sectors that may be more at risk, and those critical to the Australian economy, the Department proposes lowering the reporting threshold to include:

- entities with an annual turnover of at least $3 million
- all entities regulated under the SOCI Act.

As the intention of the obligation is to build the Australian threat picture, the Department proposes capturing entities operating in Australia, or Australian entities operating overseas where the incident has had an impact on Australia or individuals within Australia.

Timeframes for reporting

What we heard …

There was support for the proposal to report within 72 hours,[98] with submissions also recommending consistency with other regulatory reporting timeframes applicable to particular entities.[99]

Some submissions suggested staged reporting, with an initial notification of an incident within 72 hours (or as soon as possible), and a follow up report with all available information within a longer timeframe (e.g. 30 days).[100] Other submissions did not support a strict timeframe, suggesting reporting should be done as soon as practicable.[101]

A couple of submissions recommended tiered reporting thresholds based on entity size, criticality of impacted information, and requirements for information in the reporting.[102]

---

[93] See e.g., Australian Information Security Association, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, 1 March 2024 <https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/Australian-Information-Security-Association-AISA-submission.PDF> ('ASIA Submission'); Tech Council of Australia, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, 8 March 2024 <https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/Tech-Council-of-Australia-submission.PDF>, Software Alliance Submission.

[94] Australasian Higher Education Cybersecurity Service, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, 24 February 2024 <https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/Australasian-Higher-Education-Cybersecurity-Service-AHECS-submission.PDF> ('AHECS Submission'), .au Domain Administration, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, February 2024 <https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/_au-Domain-Administration-auDA-submission.pdf>.

[95] Financial Advice Association of Australia, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, 1 March 2024 < https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/Financial-Advice-Association-Australia-FAAA-submission.PDF> ('FAAA Submission'); National Australia Bank, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, March 2024 <https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/nab-cyber-submission.pdf>, Veroguard Systems, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, 1 March 2024 < https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/VeroGuard-submission.PDF> ('VeroGuard Systems Submission').

[96]See, e.g. VISA, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, 1 March 2024 <https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/Visa-submission.PDF>.

[97] Confidential submission(s) to the Department of Home Affairs.

[98] Confidential submission(s) to the Department of Home Affairs.

[99] Australian Digital Health Agency, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, 23 February 2024 < https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/Australian-Digital-Health-Agency-ADHA-submission.PDF>.

[100] Property Exchange Australia, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, March 2024 <https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/Property-Exchange-Australia-PEXA-submission.PDF> ('PEXA Submission').

[101] Confidential submission(s) to the Department of Home Affairs.

[102] Confidential submission(s) to the Department of Home Affairs.

How we responded…

The Department proposes that captured entities will be required to report within 72 hours after a ransomware or cyber extortion payment is made. This timeframe reflects feedback from industry that for ransomware and cyber extortion payment reporting, efficiency is necessary to mitigate potential ongoing repercussions.

As there are currently no other cyber incident reporting obligations that capture ransom payments, it will not be possible to acquit this reporting obligation through other cyber incident reporting obligations. This will be an additional reporting obligation only applicable where a business experiences a cyber incident, receives a ransom demand and elects to pay the ransom.

As the Department is proposing the obligation to report ransom demands will be voluntary, there is no set requirement to report within a specific period. Affected entities will be encouraged to voluntarily report as soon as practicable.

No fault, no liability

What we heard …

There was strong support for enshrining no-fault, no-liability principles within the reporting framework. These submissions stressed that these principles will be critical to encourage timely and comprehensive reporting on cyber incidents.[103] In line with the purpose of these measures, the focus should be on expanding the threat intelligence base and assisting impacted entities, not findings of fault.[104]

On the balance of principles with public expectations of accountability, submissions noted that mature entities can still suffer breaches and attacks, suggesting the public expects Government to minimise harm resulting from incidents, not attribute fault. Submissions recommended penalisation should target repeated non-compliance with reporting obligations, however organisations should not be absolved of responsibility for poor cyber security practices, particularly in the event of preventable breaches.[105]

How we responded…

The Department proposes that no-fault, no liability:

- will apply to the conduct of the government agency that receives the ransomware and cyber extortion reports and;
- would only apply to that agency's dealing with the content of the ransomware and cyber extortion reports.

Reported information subject to this no-fault, no-liability framework that is on-shared to regulatory agencies will not be able to be used for the purpose of regulation against the reporting entity. However, this is not intended to be a safe harbour, and as such, any regulators may gather information through their own legislated functions. Australia's existing laws and regulations apply to the conduct of the entity and nothing in the legislation will be construed to limit their application.

Penalties for non-compliance

What we heard …

Submissions did not oppose reasonable civil penalties as proposed, or aligned with comparable regulatory frameworks.[106] Most submissions stressed the need for proportionate penalties, and consideration for size and capabilities of entities, such as through a tiered penalty system.[107]

---

[103] See e.g., Splunk Submission; Macquarie University Submission; Australia Post, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, March 2024 <https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/Australia_Post-submission.PDF>; Cybersecurity Coalition Submission.
[104] See e.g., ACCI Submission.
[105] Engineers Australia, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, 4 March 2024 <https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/Engineers-Australia-submission.PDF>.
[106] See e.g., NCC Group, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, March 2024 <https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/NCC-Group-submission.PDF> ('NCC Group Submission').
[107] See e.g., Telstra, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, 1 March 2024 <https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/Telstra-submission.PDF>; FAAA Submission.

Some submissions suggest strong penalties including increasing fines and public reporting of non-compliance.[108] In contrast, several submissions do not support a civil penalty scheme, suggesting that incentives should be provided to report instead.[109] Others suggested alternative penalty schemes, including infringement notices,[110] education[111] and or referral to regulators for compliance audits.[112] Several submissions do not support a civil penalty scheme, suggesting that incentives should be provided to report instead.[113]

How we responded…

The Department proposes a proportionate civil penalty scheme that would encourage engagement with Government in the first instance. In the event of non-compliance, the Department would attempt an education and engagement approach in first instance. As required, an entity could be sent a reminder or formal letter, and civil fines to be issued for persistent non-compliance. This reflects feedback received through the consultation process that a punitive approach could further victimise the victim.

Sharing ransomware information

What we heard …

Submissions overwhelmingly support the sharing of anonymised, timely and actionable information on emerging and ongoing threats, as well as broader trends.

Submissions emphasised the need to ensure published information on attacks is anonymised to the greatest possible extent.[114] Time-critical information should be shared expeditiously through existing platforms to minimise harm to potentially impacted entities.[115] Submissions also support sharing of regular summaries including information on campaigns, targets, attacker behaviour and case studies of successful disruptions resulting from information sharing.[116] One submission noted that effective information sharing to industry will help establish reciprocal trust and promote reporting.[117]

How we responded…

The Department proposes information received through the reporting obligation be collated and distributed providing anonymised detail to assist entities to prepare for, respond to and bounce back from a ransomware or cyber extortion incident. The reporting data can also be used to inform updates to the ransomware playbook, and contribute to ASD's Annual Cyber Threat Report. Though the ransomware playbook is a part of the current status quo, having specific data on ransomware and cyber extortion payments can be a great value-add to industry in strengthening cyber security and in attack prevention.

---

[108] MDR Security submission; VeroGuard Systems Submission.
[109] See e.g., Ai Group Submission; Gateway Network Governance Body, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, 27 February 2024 <https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/Gateway-Network-Governance-Body-GNGB-submission.PDF> ('GNGB Submission'); PEXA Submission.
[110] Black Ink Legal Submission; FAAA Submission.
[111] Australian Financial Markets Association, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation,* Department of Home Affairs, 1 March 2024 < https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/Australian-Financial-Markets-Association-AFMA-submission.pdf.
[112] University of Queensland, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, 1 March 2024 < https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/University-of-Queensland-UQ-submission.PDF>.
[113] See e.g, Ai Group Submission; GNGB Submission; PEXA Submission.
[114] See e.g., PEXA Submission; NCC Group Submission; CISOLens, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, 29 February 2024 <https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/CISO-Lens-submission.PDF>.
[115] AHECS Submission; Insurance Council Submission.
[116] AHECS Submission; Ai Group Submission; CYAINSE, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, 25 February 2024 <https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/CYAINSE-submission.PDF>; ASIA Submission.
[117] DQS, *Submission to 2023-2030 Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation*, Department of Home Affairs, 1 March 2024 <https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative-reforms/DQS-submission.PDF; ANZ Submission.

Major decision points

Table 4. Timeframes for major decision points on the status of the IA

Decision point	Timeframe	Status of the IA
Drafting for Australia's Cyber Security Strategy 2023-2030	July 2023	Discussed with OIA the need for an IA, preparation for a draft IA commenced.
Draft consulted across Government	September 2023	Complete draft IA provided to OIA
2023-2030 Australian Cyber Security Strategy released	November 2023	Proposed measure detailed in strategy for public awareness.
2023-2030 Australian Cyber Security Strategy: Legislative Reforms consultation paper released	December 2023	Discussions with OIA on the need for a full IA, proposed measure released in detail for stakeholder feedback.
Drafting for Cyber Security Bill	March 2024	Consultation period closes, full IA drafting commenced to incorporate feedback.
Interim Government decision	April 2024	1st pass assessment completed and sent to OIA for comment.
Initial Government decision	April 2024	OIA finds 1st pass adequate, provided comment for improvement
Final Government decision	September 2024	OIA approves 2nd pass IA.

The best option and implementation

Option 3 presents the best option**:** mandatory reporting of ransomware and cyber extortion payments alongside voluntary reporting of ransomware demands and/or cyber-incidents for entities with an annual turnover of greater than $3 million. This option best balances the regulatory burden on industry and Government, with the intended benefits of generating a more complete threat picture of ransomware and cyber extortion payments in Australia. The regulatory impact analysis conducted in response to **question 4**, in combination with an analysis of stakeholder consultation conducted in response to **question 5**, shows the most support for only a single reporting obligation. Given ASD already receives a significant number of reports, there are other regulated schemes, and considering the not insignificant regulatory burden of incident reporting, a mandatory reporting obligation limited to payments of ransoms fills a critical gap in cyber threat intelligence.

Engagement Plan

The Government aims to implement the proposed measures in a way that ensures entities within the selected thresholds:

- understand and comply with their obligations
- are encouraged to engage with the Government
- receive relevant information on the ransomware and cyber extortion threat picture
- receive assistance and guidance from Government that has been enhanced by the additional data collected under these measures.

Implementation Risks

To address the risk of non-compliance with the regime, the Department will ensure that entities understand their obligations and are clear on how they can acquit them through industry engagement and guidance. Additionally, implementing a no-fault, no-liability clause will provide assurance businesses that the ransomware report will not be used in regulatory compliance action against the entity for activities undertaken in relation to resolving the ransomware attack. Government has selected the option that balances a reduced regulatory burden on industry while still acquiring essential information. Engagement and consultation on the legislation will commence prior to, and continue following, the legislation entering into force to ensure that entities are ready to meet their obligations.

There is also a Risk that Government will not be able to build a sufficient picture of the ransomware and cyber extortion threat environment when only collecting data about payments. Government will continue to analyse the incoming data and assess the strengths and limitations of Option 3 in addressing our current and future needs.

Legislation

In 2024, the Government seeks to develop cyber security legislation. This measure will be one of a suite of measures introduced through this legislation.

The mandatory ransomware and cyber extortion payment reporting obligations will commence upon Proclamation, but will be subject to a transitional period of 6 months to allow sufficient time for industry to adjust to the new obligations.

Establishing regulatory function

The Government will have to establish a new reporting function for ransomware and cyber extortion payments. While not yet settled, the Department of Home Affairs may be both the regulator and recipient of

reports. Alternatively, the ASD's ACSC may be designated the recipient of reports, retaining the Department of Home Affairs purely in a regulatory function.

There is clear precedent for a multiagency approach. For the mandatory cyber incident reporting obligations in Part 2B of the *Security of Critical Infrastructure Act 2018*, the ASD was designated the relevant Commonwealth entity to receive reports. The Department of Home Affairs retained the regulatory function for enforcing any civil penalty provisions relating to that section. Subject to further consultation, a similar approach will be adopted in these proposed measures.

The costs to Government of implementing these functions is proposed to be absorbed by the relevant agencies.

Evaluation against success metrics

Home Affairs would be responsible for implementing this recommendation, with support from the ASD. An internal post-implementation review of the mandatory ransomware and cyber extortion reporting regime should occur no later than two years after implementation in line with other measures brought forward in the same legislative package, as outlined under the 2023-2030 Australian Cyber Security Strategy.

This will ensure the ransomware and cyber extortion reporting obligations are collecting the intended information, sufficient to both support intelligence and law enforcement agencies offensive cyber operations, but also provide tailored advice to industry and Australian businesses, particularly small businesses which may feel the impact of financial losses more acutely than larger businesses. If industry and business receive consistent, tailored advice that promotes strong cyber security practices and better cyber hygiene, they will know how to proactively secure their data, systems and assets and avoid common security mistakes, such as not patching common security vulnerabilities with updates, that ransomware actors and cybercriminals can exploit. Subsequently, not only are industry and business' cyber security posture uplifted, but also that of the Australian consumer.

An informal post-implementation review may also reveal whether further reforms may be required to address the impact of ransomware demands and payments on affected stakeholders, to ensure a broad uplift in the cyber resilience of Australia, in line with the 2023-2030 Australian Cyber Security Strategy. A mix of quantitative and qualitative data should inform this review such as:

- the number of ransomware and cyber extortion reports made by industry and business to ASD
- which critical infrastructure assets are being targeted or affected by ransomware and cyber extortion demands and payments
- the impact on critical infrastructure assets being taken offline or adversely affected due to ransomware and cyber extortion demands and payments, for example, telecommunications networks or banking and financial transactions
- what variants of ransomware are being used where they have successfully been deployed in a system and data is locked or encrypted
- what ransomware actors and cybercriminals are the most active, or have had the most success in deploying ransomware and cyber extortion demands and receiving payments
- data from other mandatory reporting regimes such as mandatory cyber incident reporting under the *Security of Critical Infrastructure Act 2018*
- data from voluntary ransomware and cyber extortion reports, where a reporting entity engages with ASD or the Department of Home Affairs,
- where permissible under existing information sharing arrangements, data from other voluntary reporting regimes such as the Office of the Information Commissioner's (OAIC) cyber incident and data breach notification regime to break down Commonwealth, state and territory requirements.

Quantitative data collected will include the number of ransomware and cyber extortion payments and incidents. This would include data gathered by the regulator through the mandatory reporting. This will be supplemented by voluntary reporting, engagements and educational activities with key stakeholders, and open source research on key trends in ransomware and cyber extortion.

Measures of Success:

- By the implementation date and following the relevant transitional period, the regulator receives a number of reports on ransomware and cyber extortion payments closer to the true number of payments made, than what is currently reported voluntarily.

- Through tailored and bespoke ransomware and cyber extortion guidance, and anonymised and actionable threat reports provided to industry and business, the ransomware and cyber extortion business model is in part disrupted by industry and business' enhanced cyber security posture.
- Intelligence and law enforcement agencies successfully deploy their offensive cyber capabilities using threat intelligence informed in part by ransomware and cyber extortion reports to disrupt criminal activities in Australia and overseas, and target ransomware threat actors and other cyber criminals.