Public consultation
2023-2030 Cyber Security Strategy
Discussion Paper

Department of Home Affairs

Bupa submission

Contact:

Daniel Parsons
Director Public Affairs
Bupa Asia Pacific
33 Exhibition Street, Melbourne, 3000
E: [redacted]
W: www.bupa.com.au

About Bupa Asia Pacific

We're a healthcare leader in Australia with a purpose that sets us apart from the rest: we're committed to helping people live longer, healthier, happier lives and making a better world.

As one of Australia's largest health insurers, Bupa supports more than 4.7 million customers in their health and wellbeing. Apart from governments, health insurers are the most significant funders of health services in Australia.

We are also one of Australia's largest private providers of aged care, supporting more than 5,000 residents across 59 care homes. Our health services offering includes dental and optical providers, and contracted services to the Australian government, including responsibility for the health care delivered to Australia's Defence Force personnel, and medical checks for [relevant] visa applicants in Australia's immigration program.

The Bupa Foundation is one of Australia's leading corporate foundations dedicated to helping people live longer, healthier, happier lives and making a better world. Over the past 17 years, the Foundation has invested more than $36 million in partnerships focused on delivering programs that build mentally healthy and resilient communities, and address the link between planet health and human health.

We also recognise that the health of people is directly linked to the health of our planet, so we invest in renewable energy and waste reduction strategies to reduce our impact on our environment.

Bupa Asia Pacific is part of the Bupa Group, an international healthcare company created in 1947 with the founding purpose – 'to prevent, relieve and cure sickness and ill-health of every kind' – enshrined in our original constitution. With no shareholders, our profits are reinvested into providing more and better healthcare for the benefit of current and future customers around the world.

Executive Summary

Bupa strongly supports the Australian government in its goal to be the world's most cyber secure nation by 2030. We welcome the Expert Advisory's Board's (**Board**) discussion paper as part of their development of an ambitious, flexible, and forward-looking cyber security strategy.

With threats and challenges constantly growing and evolving in the digital world, we agree that the review of the current strategy is timely to improve our cyber resilience and security.

Given the nature of the challenges being faced by many organisations within the economy, we suggest that the draft strategy could be enhanced by:

1. Supporting small and medium-sized businesses (SMBs) in their cyber security practices; and
2. Minimising supply chain risk.

Introduction

Technology and digital innovations have revolutionised the Australian economy, changing the way we live, work, and interact as a society. Whilst it continues to present significant opportunities, it also brings enormous challenges for individuals, organisations and governments to protect themselves from malicious actors in the cyber ecosystem. We agree with the Board that *"Our national resilience, economic success, and security rely on us getting our cyber settings right."*[1]

As a healthcare leader in Australia, Bupa has embraced technologies and digital innovation to enable our customers to experience and access healthcare journeys that are simple, relevant and affordable. We moved quickly at the start of the pandemic to cover consultations and treatments delivered digitally. Our customers and healthcare providers embraced the change, and we were proud to be the first Australian health insurer to announce permanent funding for some ancillary services such as physiotherapy, psychology and occupational therapy via telehealth in 2020. We believe that greater investment in digital health and data integration is key to maximising access, productivity and innovation in the health system.

Ongoing investment in cyber security is a vital enabler of this digital innovation and connectivity. We believe our ability to deliver health care to our customers safely and maintain their information securely requires constant reflection, investment and improvement in our cyber security systems and practices. It is not simply a technological investment but rather a business one, fundamental to our success as a trusted and leading healthcare company.

Bupa makes this submission in relation to the Minister for Cyber Security's draft *2023-2030 Cyber Security Strategy Discussion Paper*, published on 27 February 2023.

We recognise that revising the strategy is timely, given increase in the number, scale and sophistication of the cyber threats face by Australian businesses, small and large. Furthermore, we agree with the Board that *"to lift and sustain cyber resilience and security, it must be an integrated whole-of-nation endeavour."*[2]

Whilst we believe the discussion paper overall is positive, we encourage the Board to consider improvements that may help the Australian Government achieve its vision of being *"the most cyber secure nation in the world by 2030."*[3]

In this submission we suggest that the draft strategy could be enhanced by:

1. Providing tangible proposals that prioritise supporting small and medium-sized businesses (SMBs) in their cyber security practices; and
2. Focusing on third- and fourth-party cyber risk for Australian organisations by fostering safe collaboration and improving the standards and resilience of software and service providers.

[1] 2023-2030 Australian Cyber Security Strategy Discussion Paper, Australian Government, 2023 available at 2023-2030 Australian Cyber Security Strategy (homeaffairs.gov.au) (page 6)
[2] Ibid. page 7
[3] Ibid. page 4

1. Supporting small and medium-sized businesses

At Bupa, we know that our customers' trust is built upon our investment in comprehensive security protections and systems that secures their data, privacy, and personal information. Furthermore, we recognise that we must prioritise our customers safety and security and agree with the Board that whilst it is companies that are impacted by cyber security breaches, *"it is their customers who are the real victims of these insidious crimes."*[4]

Rather than shying away from technology, Australians have embraced the digital world and all its opportunities. They expect organisations such as Bupa to help facilitate and accelerate this by offering technological advancements in our services and products. However, innovation in our services and expansion in digital technologies is only possible because of our focus on protecting our customer's information and continually improving and strengthening our defences against potential cybersecurity breaches.

We are concerned that the proposed strategy focuses too heavily on creating more requirements and penalties without offering proposals that support SMBs in improving their cybersecurity capabilities. Australian organisations are facing threats and attacks from cyber criminals that are increasingly sophisticated, adaptable, and adept in their endeavours to exploit our people and our cyber security systems. According to the Australian Cyber Security Centre's (ACSC) *July 2021 – June 2022 Annual Cyber Threat Report,* one incident is reported on average every 7 minutes with more than 76,000 cybercrime reports in the relevant period.[5]

In recognition of this, Australian businesses are dedicating an increasing portion of their operating budget towards making their cyber systems more resilient and secure. In 2020, approximately $5.6 billion was spent nationally on cyber security, with this figure expected to reach $7.6 billion by 2024.[6] However, we are concerned that the safeguards necessary and the continual investment required is becoming increasingly expensive, inaccessible, and difficult for SMBs to implement. This is of particular concern given that 99.8% of Australian businesses are SMBs, contributing more than half our national GDP.[7] Most SMBs have considerably less resources and capacity to manage their business and cyber security systems, with 97% of Australian businesses having less than 20 staff.[8] As a result, it is important to support these businesses in their security efforts as the nature of cyber threats continue to evolve.

In the ACSC's 2019 survey of more than 1700 Australian SMBs, it concluded that organisations know the importance of cyber security and investing in best practice processes, however face significant barriers to implement the necessary safeguards and security practices.[9] One barrier is financial constraints, with nearly half (48%) of SMBs surveyed reporting that they spent less than $500 on cyber security per year,[10] the OECD labelling this "less than optimal".[11] This is despite the fact that medium-

[4] 2023-2030 Australian Cyber Security Strategy Discussion Paper, Australian Government, 2023 available at 2023-2030 Australian Cyber Security Strategy (homeaffairs.gov.au) (page 7)

[5] Australian Cyber Security Centre. (2022). ACSC Annual Cyber Threat Report, July 2021 to June 2022. Available at ACSC Annual Cyber Threat Report, July 2021 to June 2022 | Cyber.gov.au

[6] AustCyber. (2020) Australia's Cyber Security Sector Competitiveness Plan: 2020 Update (Chapter 1: The Australian cyber security sector today). Available at SCP - Chapter 1 - The Australian cyber security sector today | AustCyber

[7] Commonwealth Scientific and Industrial Research Organisation. (2022). SMEs key to driving growth in Australia Simon Hanson, CSIRO SME Director. Available at SMEs key to driving growth in Australia Simon Hanson, CSIRO SME Director - CSIRO

[8] Australian Cyber Security Centre. (2020). *Cyber Security and Australian Small Businesses: Results from the Australian Cyber Security Centre Small Business Survey*. Available at Small Business Cyber Security | Cyber.gov.au

[9] Ibid.

[10] Ibid.

[11] Organisation for Economic Cooperation and Development (OECD) (2020): Digital Security and Data Protection in SMEs: How to ensure SMEs are less vulnerable for a post-COVID digital world? Summary of Proceedings for Digital

sized businesses (defined by the Australian Bureau of Statistics as between 20 and 199 employees) had the highest average loss per cybercrime report ($88,000) of all organisation sizes, where a financial loss occurred.[12]

A second barrier is expertise, with many SMBs having a lack of knowledge to properly mitigate cybersecurity risks themselves, or to ensure they are properly protected when outsourcing security measures. In terms of taking responsibility for cybersecurity, 97% of sole traders and 65% of small businesses (2 to 19 employees) manage it themselves, despite the fact that 60% of SMBs rate their understanding of cybersecurity as 'average' or 'below average'.[13]

For these reasons we believe it is vital the Australian government develops a strategy that provides practical support to SMBs in uplifting their cybersecurity capacity. The ability of these providers to protect themselves is challenged by compliance and implementation costs, and helping these businesses become more cyber resilient will reduce risk across the whole digital economy.

We suggest the Board explore ways to enable organisations to collaborate and work securely with third parties to help them meet their regulatory obligations without adding an undue financial burden. We suggest that rather than focusing on penalties and enforcement, the strategy consider the implementation challenges for SMBs and how these can be overcome. Furthermore, we believe there needs to be a focus on improved information and threat sharing to ensure greater resilience in the cyber environment. By better supporting and incentivising SMBs to uplift and invest in their cybersecurity efforts, we can help reduce the risk of cyberattacks across the Australian economic landscape and keep the community safe.

2. Minimising supply chain risk

Organisations across Australia work with multiple external vendors, contractors and service providers to deliver goods and services. Whilst this increases efficiency and enables them to provide higher quality products to consumers at lower prices, it also introduces some risk to the business via third parties and beyond in the supply chain. Third parties are those who are directly connected to the original organisation, whilst fourth parties are those that are connected to the third-party organisation.[14] This complexity results in a lack of visibility for large organisations into the business policies and security standards of the parties they partner with. As a result, this can make it difficult to assess risk, vulnerabilities and ensure cyber resilience in supply chains.[15]

At Bupa, we believe that managing cyber risk is critical to our ability to deliver quality healthcare services for all our customers.[16] We have both a responsibility to protect our customers' data, and the capacity to invest in strengthening and safeguarding our digital security systems. However, we are concerned about the cyber threat landscape and its evolving nature. These concerns are not unique, with more than 92% of Australian businesses reporting that they expect a cybersecurity incident to disrupt their business in the next 12 to 24 months.[17]

for SME 'D4SME' Global Initiative webinar. Available at D4SME Digital Security and Data Protection Webinar Summary Record.pdf (oecd.org)

[12] Australian Cyber Security Centre. (2022). ACSC Annual Cyber Threat Report, July 2021 to June 2022. Available at ACSC Annual Cyber Threat Report, July 2021 to June 2022 | Cyber.gov.au

[13] Australian Cyber Security Centre. (2020). *Cyber Security and Australian Small Businesses: Results from the Australian Cyber Security Centre Small Business Survey*. Available at

[14] Graham Kaitlyn, BitSight. What is Third-Party vs. Fourth-Party Risk? And How to Manage Both (13 December 2022). Available at What is Third-Party vs. Fourth-Party Risk? And How to Manage Both | BitSight

[15] Miklovic, Dan, Whitty, Roberta J. Case Study: Cisco Addresses Supply Chain Risk Management (17 September 2010) Available at What Is SCRM - Supply Chain Risk Management? - Cisco

[16] Bupa. Security and Fraud Protection. Available at Security and fraud protection| Bupa

[17] CISCO (2023) Cisco Cybersecurity Readiness Index: Resilience in a Hybrid World (Australia edition). Available at cybersecurity-readiness-market-snapshot-australia (cisco.com)

As a large organisation, Bupa is often at the centre of a vast data ecosystem, partnering with many service providers and third parties to deliver services to our customers and manage our operations which help our customers live longer, healthier, happier lives. Working with experts enables us to deliver social and economic benefits to the community. It does, however, increase our organisation's overall risk profile. This is because to form effective and collaborative partnerships, we are required to share customer data with third parties (many of which are SMBs) but have a lack of control and oversight of their cyber security practices and safeguards.

Given the increasingly sophisticated and rapidly evolving nature of cyber threats, the lack of transparency and protection for third parties reduces our ability to operate efficiently and safely. This lack of third-party resilience is particularly problematic for private health insurers, given the heightened risk of cyber breaches experienced in the heath sector. According to the Office of the Australian Information Commissioner, the healthcare industry was the most targeted by cybercriminals in Australia in the second half of 2022, reporting 14% of 497 data breaches.[18]

Attacks through our third parties exposes our organisation to breaches that may not only negatively impact our reputation but can ruin our customer's trust and even cause harm to vulnerable individuals and communities. Furthermore, it is important to recognise that Australia's health system is a complex network of stakeholders and suppliers, which large private health insurers work with daily to support their members. Many of these are not suppliers in the traditional sense but integral stakeholders we are required to partner with to successfully deliver an end-to-end health insurance product that provides customers with a seamless and interconnected health care journey. Thus, the impact of cybercrime can have wide-reaching ramifications that are not just financial but also damage the Australian health ecosystem.

We suggest that it would be appropriate to consider strategies for encouraging safe collaboration and threat intelligence sharing with third parties. This would allow larger organisations to manage their third-party relationships and cyber risks more effectively. It would also allow greater levels of support for SMBs to strengthen their defences to increase cyber resilience. Information sharing and helping our third-party partners enhance their security measures is critical to reduce the risk of future cyber breaches across the economy, defend against attackers and better secure supply chains.

Bupa agrees with the Board that *"To be the most cyber secure nation in the world by 2030, Australians should have confidence that digital products and services sold are fit for purpose and include appropriate best practice cyber security protections."*[19]

Despite this statement however, we are concerned that the draft strategy is largely silent on supply chain risk for large organisations, particularly the resilience of third-party service providers and the insecure software products and services they may rely upon. Many SMBs, acknowledging their lack of expertise in the cybersecurity space, choose to outsource their protection. In the small business survey discussed previously, the ACSC found that 41% of medium-sized businesses chose to outsource their cyber security measures.[20]

Although this appears preferable, this may instead lead to increased vulnerability for these organisations as they are not necessarily as protected as they believe they are.[21] This creates a situation where despite their best intentions, third parties may not be aware of their cyber vulnerabilities,

[18] Office of the Australian Information Commissioner. (2023). Notifiable data breaches report: July to December 2022. Available at Notifiable Data Breaches Report: July to December 2022 | OAIC

[19] 2023-2030 Australian Cyber Security Strategy Discussion Paper, Australian Government, 2023 available at 2023-2030 Australian Cyber Security Strategy (homeaffairs.gov.au) (page 17)

[20] Australian Cyber Security Centre. (2020). *Cyber Security and Australian Small Businesses: Results from the Australian Cyber Security Centre Small Business Survey*. Available at

[21] Ibid.

thus exposing themselves and their partners to malicious attackers. This increases systemic risks across the entire digital ecosystem, leaving ordinary Australians to suffer the consequences.

To improve the standard and incentivise safe and secure software development, we suggest the strategy broaden its scope to consider the legal framework, including compliance and liability, for consumers of insecure software products and services. We believe there should be minimum security standards for SMBs and software providers to help protect Australian organisations and consumers. In conjunction with greater collaboration, this would incentivise high cyber security standards and best practice software security from manufacturers and vendors, ensuring that the consequences of cyber breaches are not born by Australian consumers.

Conclusion

Technological advancements and digital innovation have changed our world, delivering extraordinary benefits to all Australians. However, the growing digital environment and our reliance on increased connectivity has presented criminals and nation states with new opportunities to exploit and harm everyday Australians. Cyber-enabled crime is a growing threat, and whilst everyone has an essential role in securing our economy, we agree with the Board that *"We need a coordinated and concerted effort by governments, individuals, and businesses of all sizes."*[22]

Bupa supports the government in its goal to ensure Australia is a world leader in cyber security. Given the rapidly evolving cyber landscape and acceleration in digital innovation, it is a difficult task to form a cyber security strategy that is fit-for-purpose not only today, but that is forward-looking to 2030. A strategy that prioritises support and practical measures to meet the compliance and implementation challenges this may create is imperative to ensuring cyber resilience across all levels of the digital economy. Whilst penalties and enforcement are important, ensuring that implementation costs are not prohibitively expensive, enabling greater information and threat sharing, and fostering collaboration will lead to improved transparency, reporting and overall cyber security.

For ideas regarding the matters discussed in this submission, we also encourage the Board to review the US National Cybersecurity Strategy released on 2 March 2023 to more closely examine how it suggests using market forces to promote security and resilience.

We are pleased that in their discussion paper, the Board is looking to actively collaborate with the community, organisations, and experts to craft a strategy that is comprehensive, inclusive, strong and flexible. We thank you for the opportunity to contribute, both through this submission and via discussions with our Chief Information Security Officer, John Ellis. We hope you find our engagement meaningful and welcome the opportunity to provide further input and feedback throughout the process.

[22] 2023-2030 Australian Cyber Security Strategy Discussion Paper, Australian Government, 2023 available at 2023-2030 Australian Cyber Security Strategy (homeaffairs.gov.au) (page 7)