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

Table of Contents

14 May 2023

Mr Andy Penn AO
Chair
Expert Advisory Board
Department of Home Affairs

Dear Mr Penn,

Visa's response to the 2023-2030 Australian Cyber Security Strategy: Discussion Paper

Visa welcomes the opportunity to share its perspectives on the 2023-2030 Australian Cyber Security Discussion Paper (the Paper).

We share the Government's commitment to make Australia a world leader in cyber security, which is particularly important given the recent cyber incidents that have impacted supply chains and infrastructure, governments, and large and small businesses in various parts of the world.

In responding to this consultation, our submission focuses on several topics, including the three lenses through which Visa approaches the security of our network: cyber security, operational resilience, and fraud prevention. In addition, we provide our perspectives on a number of specific questions in the Paper, such as actions which would assist in making Australia the most cyber secure nation in the world by 2030.

Visa is available to provide further details on our submission if helpful.

Yours sincerely,

[redacted]
Julian Potter
Group Country Manager, Australia, New Zealand & South Pacific

Overview

Cyber security is a top concern for both the private and public sectors, driven in large part by an increasingly connected and digital world. In 2021, 79 per cent of breaches globally were executed by organised crime, often via social (phishing), hacking (use of stolen credentials), and malware (ransomware)[1]. In the first half of 2021, malicious or criminal cyber-attacks remained the leading source of data breaches in Australia, accounting for 65 per cent of notifications under the Notifiable Data Breach Scheme, with ransomware incidents increasing by 24 per cent[2].

For Visa specifically, cyber security is a top priority – so we can ensure that consumers and businesses can pay and be paid with confidence. Visa invests heavily in our cyber security program, including ensuring we have the talent, tools, and state of the art technological capabilities to detect and prevent cyber attacks on our systems. Beyond our risk products and services, we work with industry organisations to develop and support standards for payment data security. In addition, we partner with clients, businesses, governments, and law enforcement agencies to help identify fraud and share security best practices and threat intelligence.

In addition, governments play an important role in ensuring cyber security. In this regard, Visa supports a cyber security policy environment that promotes a flexible and risk-based approach to cyber security. Given the importance of public-private cooperation in ensuring the security of the global payments ecosystem, we endorse the World Economic Forum's (WEF) Cyber Resilience Playbook for Public-Private Collaboration[3] as a basis for evaluating the impact of policy options for cyber security.

Beyond engagement with individual governments, Visa experiences first-hand the benefits of international collaboration in cyber security, leading to fast and frictionless information sharing across borders, for the benefit of all ecosystem participants and the customers they serve. Initiatives such as the European Cyber Resilience Board (ECRB) and the Financial Services Information Sharing and Analysis Center (FS-ISAC) in the United States involve multiple organisations working together through formal contractual arrangements and informal partnerships – across both the public and private sectors – to achieve greater global resilience to cyber attacks.

---

[1] Verizon (2022) "2022 Data Breach Investigations Report", www.verizon.com/dbir

[2] Office of the Australian Information Commissioner (2021) "Data breach report highlights ransomware and impersonation fraud as concerns", https://www.oaic.gov.au/updates/news-and-media/data-breach-report-highlights-ransomware-and-impersonation-fraud-as-concerns/

[3] World Economic Forum, Cyber Resilience: Playbook for Public-Private Collaboration, found at: http://reports.weforum.org/cyber-resilience/

Such initiatives are based on a foundation of mutual trust, where information sharing on sensitive cyber attacks is not only seen as mutually beneficial, but mutually critical in order to protect end-users across the ecosystem. Visa believes the model of collaboration across financial services to combat cyber threats is the right one, and the industry's resilience as a whole stands to benefit by better protecting it against threats of an increasingly global nature. We are committed to working collaboratively with our clients and wider industry partners to achieve a resilient global system for the customers they serve.

In addition, we believe that cyber security frameworks should:

1. **Be flexible and allow room for companies to tailor defences** based on business needs. Given the ingenuity of hackers and the fast-changing nature of cyber threats, it is vital that cyber defences quickly evolve to keep ahead of potential attacks. Static cyber policies that do not adapt to marketplace and technological developments, do little to deter cyber criminals from conducting harmful activities.
2. **Be based on globally accepted standards**. International standards form the backbone of the digital payments industry, enabling ubiquity by maximising global interoperability and acceptance across digital payments systems. In addition, whether is it ransomware, eSkimming, Distributed Denial of Service attacks or changes in the cyber crime underground, global standards underpin basic data security hygiene.
3. **Allow businesses to determine data storage practices based on business requirements**. Data is a lynchpin of the modern global economy, with digital trade contributing to economic growth and development. Digital trade barriers, including localisation requirements, can have unintended consequences, potentially harming cyber security by introducing vulnerabilities into otherwise secure global systems.
4. **Encourage transparency and information-sharing** regarding threats, vulnerabilities, and controls between government and private industry, among government agencies, and between governments of different nations. Governments can also lead in the investigation and prosecution of cyber criminals to help eliminate "safe havens" and facilitate public awareness and education of cyber security efforts.

Furthermore, Visa approaches the security of our network through three lenses: cyber security, operational resilience, and fraud prevention:

1. Cyber security

Visa strongly supports focusing on strengthening defences against cyber attacks. In advancing this goal, we encourage the use of existing best-in-class industry standards to guide any future guidelines related to cyber security and fraud prevention.

In Australia and globally, Visa takes seriously its shared responsibility to help secure the payments ecosystem against cyber threats and continually improves capabilities that enable individuals, businesses, and economies to thrive. To manage the constantly changing threat environment and growing demands on our infrastructure, we devote significant resources to our talent and

technology. Visa invested US$10 billion (A$14.95 billion) in technology over the past five years, including to reduce fraud and improve security. This extends to the implementation of zero trust architecture[4], adoption of a defence-in-depth[5] approach, innovated world-class technologies, best-in-class cyber security protocols, and employment of over 1,000 world-class cyber security professionals.

Examples of key payments industry initiatives Visa has strongly advocated for as preventative measures against cyber security threats include: (i) the introduction of tokenisation for payments and (ii) support for the Payment Card Industry Data Security Standards (PCI DSS)[6]. Both initiatives have provided industry participants with additional layers of security to protect against the potential compromise of sensitive data such as payment credentials.

2. Operational resilience

There are synergies between operational resilience and cyber resilience, and a more aligned approach will better protect the ecosystem and bolster the resilience of the global infrastructure in which we operate. Even when their root causes differ, the impacts, the recovery, and the response activities associated with a range of failure types can overlap significantly. The more Australia's approach to cyber and operational resilience can be aligned, where appropriate, the better the outcome for end-users.

Given the role of Visa's network in supporting global commerce, it is fundamental to our mission that we have a resilient global platform. VisaNet is our global technical architecture involving multiple data centres around the world. The ability to route transactions through multiple data centres, as needed, significantly increases our resilience and capacity. VisaNet has successfully processed more than 99.999 per cent of transactions it has received over the last five years.

Furthermore, in an environment where more people than ever are turning to digital payments, there has never been a more important time for Visa to collaborate with our clients and the broader industry to enhance the payments ecosystem's approach to operational resilience.

Looking forward, a flexible approach is essential to enable payments ecosystem participants to tailor their approach to their specific business services, customer needs and ecosystem

---

[4] Definition of zero trust architecture: An enterprise's cyber security plan that utilises zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture plan. See: Zero Trust Architecture - Glossary | CSRC (nist.gov)

[5] Definition of defence in depth: Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organisation. See: defense-in-depth - Glossary | CSRC (nist.gov)

[6] PCI Security Standards Council (2021) "Updated PCI DSS v4.0 Timeline" https://blog.pcisecuritystandards.org/updated-pci-dss-v4.0-timeline

interdependencies, and in turn deliver the appropriate resilience outcomes. This should be aligned to commonly agreed principles, to ensure a minimum standard that customers can expect. Well-designed and technology-neutral standards created by the international standards community are typically more agile, flexible, and 'future proof' than rules-based, prescriptive regulation. This can be a powerful way to drive best practices, minimise risks, and build interoperability – both technical and legal.

It is critical that a principles-based approach is adopted that allows individual firms the flexibility to define appropriate tolerance metrics and levels. A one-size-fits-all approach would not be reflective of the disparate nature of activities and approaches of different companies. Even within individual companies, Visa would expect there to be multiple impact tolerance levels, which would vary depending on the nature of different services provided.

3. Fraud prevention

Visa is focused on maintaining relationships with our clients, employees, and stakeholders based on integrity and trust by respecting individual privacy rights and protecting the personal information entrusted to us. We use Artificial Intelligence (AI) and machine learning to analyse approximately 500 unique risk attributes of any transaction, including critical information about the device, account holder spending profiles, and global fraud trends. This fraud prevention system helps financial institutions identify and respond to emerging fraud patterns and trends globally in real-time, making the global payment ecosystem safer for retailers and consumers. In 2022, Visa's fraud prevention tools helped prevent approximately US$27 billion (A$39 billion) in fraud.

Visa relies on layers upon layers of security technologies to protect the valuable data flowing through our system. This multi-layered security approach has kept fraud rates low, despite significant growth in transaction volumes. We conduct regular exercises to ensure that in the event of an incident, we are fully prepared to respond effectively and expeditiously.

Visa has a number of guardrails in place to protect consumers. Having rolled out chip cards in Australia (and progressively across the world), we have made it virtually impossible for cyber criminals to take stolen account numbers and create counterfeit cards that can be used in stores with EMV Chip terminals. We are also devaluing data by removing the static 16-digit primary account number from the payment process through technologies such as tokenisation, so that there is no card number out in the open for criminals to steal. Alongside these practices, Visa uses sophisticated data analytics and risk monitoring to ensure that, when a consumer dips their card or enters a card number into an e-commerce site, it's the account holder and not a criminal.

Visa provides below its responses to specific questions included in the Paper.

Response to specific questions

1. What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

In addition to the recommended approaches outlined above, Australia will enhance its prospect of being the most cyber secure nation in the world by 2030 through both government and industry undertaking the following actions:

- Adopt zero trust architecture that is based on the concepts of a perimeter-less network, least privilege and limited lateral movement as well as applying zero trust approaches regarding increased transparency, oversight, and governance.
- Implement a defence-in-depth approach that drives a model of multiple layers of protection that can prevent a single point of failure.
- Focus on delivering products that are built with security by design in mind.
- Invest in automation, AI and machine learning in the areas of threat detection and response.
- Invest in supply chain risk management by applying AI and machine learning to Network Behaviour Anomaly Detection / Network Detection and Response (NBAD/NBR).

These actions will help place Australia at the forefront of being the most cyber secure nation in the world by 2030 as well as defending itself against ever-evolving cyber threats and improve resilience in the cyber ecosystem.

2. What legislative or regulatory reforms should Government pursue to: enhance cyber resilience across the digital economy?

The Government should continue to implement the Security of Critical Infrastructure (SOCI) Act and provide clarifying guidance as needed, but further legislation or regulation does not appear necessary at this time, given the robust requirements already in place for national critical infrastructure under the SOCI Act and existing obligations for a broader set of companies to take reasonable steps to protect the personal information of Australian citizens. Visa also encourages the Government to avoid specific technological mandates as such requirements can quickly become obsolete given the dynamic nature of cyber activities.

a. What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy (e.g. legislation, regulation, or further regulatory guidance)?

As noted above, Visa assesses that further legislation or regulation is not necessary at this time. However, further regulatory guidance may be helpful, particularly as best practice. Legal requirements and regulation should avoid being overly prescriptive as to particular solutions. A risk-informed, context-specific, and objective-based approach is more likely to survive the changing technical and threat landscape.

b. Is further reform to the Security of Critical Infrastructure Act required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?

In Visa's view, the SOCI Act and the existing privacy laws[7] should be sufficient to cover both the systems critical to Australian society as well as the sensitive personal data of Australian citizens.

c. Should the obligations of company directors specifically address cyber security risks and consequences?

Generally, a company's board of directors is ultimately responsible for that company's overall risk posture, including cyber security risks, and oversees implementation of a cyber security risk management program. To avoid duplicative, conflicting, or unnecessary oversight, any legislative or regulatory reforms should consider existing corporate and banking laws and standards already in place. For example, in Australia, Prudential Standard CPS234 on Information Security requires boards of a regulated entity to take responsibility for that entity's cyber security[8].

In cases where companies are based outside of Australia, legislative or regulatory reforms should recognise a company's compliance with its home jurisdiction obligations.

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

In Visa's assessment, a Cyber Security Act is not required at this time, given our response to Question 2b above. If a new Cyber Security Act is considered, Visa recommends that the Government continue to work with the private sector, allowing industry stakeholders to provide inputs prior to the enactment of such Act. At a high level, a Cyber Security Act should set baseline standards for entities within Australia not operating critical infrastructure assets to avoid duplicating existing legal requirements, such as those in the SOCI Act. In addition, a Cyber Security Act should reference consistent international standards, such as those issued by ISO and NIST, as is the case with the SOCI Act and proposed SOCI Act Risk Management Program Guidance.

e. How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to cyber security, and are there opportunities to streamline existing regulatory frameworks?

Continued engagement with industry on regulatory burden and tracking ongoing regulatory cyber security developments around the world is key. Companies that operate in multiple

[7] Privacy Act 1988 and Privacy Principle 11

[8] See cps_234_july_2019_for_public_release.pdf (apra.gov.au)

countries are, in particular, increasingly subject to often overlapping and potentially conflicting obligations concerning cyber security. As a result, it is beneficial for cyber security regulations to align to widely-accepted international cyber security standards and avoid prescribing particular technological solutions to cyber threats. To the extent Australian requirements may depart from these international standards, the guidance should clearly indicate the differences and explain the objectives of such differences. Similarly, enabling multinational companies to use existing documentation and processes to meet Australian requirements will help manage regulatory requirements.

Visa notes recent advice that the Reserve Bank of Australia (RBA) will extend its supervision to include payment systems where an outage could cause significant economic disruption and damage confidence in the financial system. This will include retail payment systems that the Government has declared to be critical infrastructure. The RBA has stated that it is engaging closely with other regulators "to ensure that the regulatory burden on the industry is minimised"[9]. While this dialogue is welcome, Visa would encourage an approach which takes account of ongoing engagement between regulators as reporting requirements potentially evolve to ensure that the regulatory burden does not expand without full and proper consideration of the impact on businesses.

f. Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by: (a) victims of cybercrime; and/or (b) insurers? If so, under what circumstances?
(i) What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies and insurers?

Government should discourage, but not prohibit, ransom payments to ensure stakeholders, including law enforcement, have the maximum flexibility to manage these attacks and protect vital interests.

g. Should Government clarify its position with respect to payment or nonpayment of ransoms by companies, and the circumstances in which this may constitute a breach of Australian law?

Yes, further clarification of the Government's position on this issue would be helpful. In addition, please see response to Q2f above.

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

Public-private partnerships that work collectively and collaboratively across industry and government to proactively share information are critical to fighting cyber crime and threats, allowing two-way sharing of information between the private and the public sector about root causes, incidents and threats. Visa recommends that Australia build on existing efforts, such as

[9] See The Reserve Bank of Australia (2023) The Shift to Electronic Payments – Some Policy Issues | Speeches | RBA

the ACSC's Partnership Program and engagements with trusted intelligence-sharing communities/initiatives, to share reliable, contextualised technical intelligence (indicators of compromise) via a centralised threat intelligence platform, with members pushing and pulling intelligence in close to real-time for the wider community's benefit. It is also important for the Government to have streamlined policies allowing for the provision of security clearances to enable private sector participation when sharing sensitive cyber security threat information.

8. During a cyber incident, would an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) improve engagement with organisations that experience a cyber incident so as to allow information to be shared between the organisation and ASD/ACSC without the concern that this will be shared with regulators?

Visa expects that assurances of confidentiality will make industry more likely and willing to share information with ASD in the event of a cyber incident.

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

Increasing public understanding of the nature and scale of ransomware or extortion demands is an important goal, but a voluntary sharing model better enables trusted collaboration between industry and government than an expanded mandatory reporting regime. Voluntary models allow incident responders to focus resources on the incident at hand rather than focusing on complying with additional reporting requirements.

10. What best practice models are available for automated threat-blocking at scale?

The sharing of contextualised, actionable threat intelligence to relevant cybersecurity vendors, and internet service and cloud providers can help protect the ecosystem at scale. Automated threat blocking is challenging given the wide range of indicator reliability and contextualisation. Automated blocking using poorly tuned indicators may result in an overabundance of false positives or unusable systems, which would ultimately result in worse overall security.

13. How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?
a. Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?

The Government should consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators. Any steps to streamline the reporting process and harmonise requirements will help network defenders focus on remediation rather than reporting to multiple regulators. In this regard, please also see Visa's response to Q2e above.

14. What would an effective post-incident review and consequence management model with industry involve?

Effective post-incident review and engagement models: (1) occur in confidential channels, (2) focus on root cause and process enhancement rather than attributing fault, and (3) focus on significant cyber incidents. Regarding this final point, this is important because the same people who need to contribute to a post-incident review also need to undertake daily cyber security functions for companies that are victims of cyber security attacks. As a result, a post-incident review for minor incidents is not advisable. Visa recommends that the Government work closely with industry participants to define which types of incidents will require after-the-fact review.

15. How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime? a. What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?

Government and industry can collaborate to generate and promote best-practice guidance with practical steps - such as how to securely configure a public cloud environment - to enable even small businesses with limited information technology resources to benefit. Additionally, making key cyber security services and capabilities available at low-to-no cost for small business can help. This can include making unique government capabilities available open source or by making government-funded cyber security services available to small business who may not otherwise be able to afford them.

16. What opportunities are available for government to enhance Australia's cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?

Australia could enhance the cyber security technologies ecosystem by providing grants, contracts, or other support to companies innovating new cyber security solutions as well as working with such companies to pilot new programs to research and develop early-stage cyber security capabilities.[10] In addition, many of these tools are too expensive or difficult for small companies without cyber security expertise to implement. As a result, government support for small business in particular may help support the uptake of cyber security services and technologies in Australia.

---

[10] For example, the United States Department of Energy funded the early development of a new threat intelligence sharing platform for the energy sector, which was later incorporated into a commercial product. In addition, the US National Science Foundation provides funding for research and development, as well as education and workforce development programs in cyber space. In the United Kingdom, the National Cybersecurity Centre has created a NCSC for Startups to provide NCSC expertise and guidance to emerging companies and a "Cyber Invest" program to partner private and government funding for cyber security research in UK universities.

17. How should we approach future proofing for cyber security technologies out to 2030?

The best way to approach future proofing for cyber security technologies is to focus on risk-based and flexible frameworks or processes and encourage innovation of new capabilities, rather than mandating specific or highly prescriptive technical solutions.

18. Are there opportunities for government to better use procurement as a lever to support and encourage the Australian cyber security ecosystem and ensure that there is a viable path to market for Australian cyber security firms?

Government can require that external vendors selling goods or services to the Government adhere to cyber security best practices. Government can also provide early-stage research and development funding and opportunities to test new capabilities for innovative cyber security firms.

19. How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?

Highly prescriptive regulatory requirements early in a product's development cycle risk limiting innovation and the creation of new technology. The best way to address the cyber security of emerging technologies and promote security by design without impeding innovation would be for the Government to:

- share best practices for secure coding and other secure design techniques;
- publicly encourage security by design principles; and
- leverage its procurement powers to require government vendors to adhere to these principles.

About Visa

Visa's mission is to connect the world through the most secure, reliable, and innovative payment network – enabling individuals, businesses, and economies to thrive. Our advanced global processing network, VisaNet, provides secure and reliable payments around the world, and is capable of handling more than 65,000 transaction messages a second.

In Australia, Visa has offices in Sydney and Melbourne. Together with our Australian financial institutions, fintech and business clients, and our technology partners, we are committed to building a future of commerce that fosters Australian economic growth, security and innovation.

Visa continues to expand acceptance across the payments ecosystem, ensuring that every Australian can not only pay, but also be paid in a convenient and secure way. Visa invested US$10 billion (A$14.95 billion) in technology over the past five years, including to reduce fraud and improve security. In 2021, Visa's AI-driven security helped financial institutions prevent more than AU$354 million in fraud from impacting Australian businesses[11].

As commerce moves rapidly online, Visa recently released its updated Australian Security Roadmap 2021-23[12] in response to the increasing risk of cyber crime and scams facing Australian businesses and consumers. The roadmap highlights the steps that Visa, together with industry, are taking to continue to secure digital payments in Australia, including:

- Preventing enumeration attacks through new ecommerce requirements
- Driving adoption of secure technologies
- Securing digital first payment experiences, including contactless ATM access
- Enhancing the cyber security posture of payments ecosystem participants
- Preventing Australian consumers and businesses from becoming victims of scams
- Ensuring payments ecosystem resilience through real-time AI solutions.

The Australian Security Roadmap 2021-23 is available here.

[11] Visa (2021) Visa's AI prevents more than $350 million in fraud from disrupting Australian businesses.
[12] Visa (2021) Security Roadmap 2021-23: Securing the Commerce Ecosystem in Australia.