eftsure

eftsure Pty Ltd
ABN 21 168 403 736
ACN 168 403 736

Level 6, 122 Walker St
North Sydney 2060
1300 985 976
www.eftsure.com

Dear sir/madam,

Re: 2023-2030 Australian Cyber Security Strategy, Discussion Paper,

Eftsure welcomes the opportunity to comment on the delivery of a forward-looking strategy, one that fortifies Australia's overall cyber posture into 2030.

About Eftsure
Eftsure is an Australian platform that specialises in payment fraud prevention. Specifically designed for business payments, Eftsure's solution uses multi-factor verification to mitigate organisations' risks of being impacted by cyber-crime, fraud or error.

Background
Many organisations' cybersecurity strategies focus on preventing system infiltrations via firewalls, anti-virus software and other backdoor protection solutions. Rightfully, security teams work to protect the confidentiality, integrity and availability of systems, devices and information. However, the vast majority of cyber-crimes (83%) reported to the Australian Cyber Security Centre (ACSC) over the last 12 months were financially motivated, according to the ACSC's Annual Cyber Threat Report 2022.[1]

Despite this trend, many organisations still protect their financial assets through manual processes that depend on staff detecting business email compromise (BEC) attacks and other social engineering tactics. These tactics are increasingly sophisticated, particularly with advances in generative artificial intelligence (AI). Further, few AP employees are specialists in fraud detection, and many traditional controls cannot protect against digital fraud attempts.

The role of payment protection
Eftsure's business-to-business payment solution updates analogue approaches to financial controls, drawing on an ever-growing, proprietary database of independently verified supplier information. Before funds are irretrievably released, Eftsure verifies electronic funds transfer (EFT) details via three-way matching between an account name, Bank-State-Branch (BSB) number and Australian business number (ABN).

[1] Australian Cyber Security Centre (2022). *Annual Cyber Threat Report 2021–22*. Accessed at www.cyber.gov.au

Eftsure welcomes the recent push for stronger anti-fraud measures, including the introduction of products like Commonwealth Bank's NameCheck or the Reserve Bank's recommendation to leverage PayID. However, these solutions tend to be more suitable for consumers rather than businesses or large organisations. This is because the products are often working from a limited pool of data and lack the batching functionality necessary to keep up with the speed and volume of payments processed by larger organisations.

By contrast, Eftsure's solution scales across any volume of digital payments. In fact, its cross-matching capability becomes even stronger as the database of verified suppliers grows. This allows it to function as both a final preventive measure – protecting the assets that most cyber-crimes are ultimately targeting – as well as a deterrent for fraud attempts. Similar to the concept behind neighbourhood watch, knowing that an organisation belongs to the Eftsure network can act as a deterrent to dissuade malicious actors from attempting to defraud its financial professionals, all while adding technical layers of security if fraud attempts do occur.

Like running antivirus software or any other common cybersecurity measure, payment protection software is not a panacea. In the same way that antivirus software is essential to include on all business computers, payment protection software is critical to the payment function of a business. It is a single yet crucial layer of defence that should be aligned with additional, cross-functional solutions.

Overview

As a business committed to preventing payment fraud, Eftsure has a keen interest in approaches that minimise organisations' exposure to financially motivated cyber-crimes, which constitute the bulk of reported cyber incidents.

As a result, this consultation examines both strategic and tactical shifts to strengthen Australia's security posture, with an overarching focus on the concept of "collaborative cybersecurity":

1. The meaning of collaborative cybersecurity and why it should be included in the Strategy
   a. Why more collective, less atomised approaches are necessary to counterbalance threat actors' growing number of advantages
   b. What collaborative cybersecurity should look like from strategic and operational standpoints
   c. Specific steps the public sector can take to model collaborative cybersecurity and other best-practice security approaches
2. The importance of prioritising prevention and how it can help government support the uptake of cyber security services and technologies in Australia

3. Why balancing automation and human oversight is crucial to automated threat-blocking at scale, as well as incentives government can consider to improve uptake of relevant practices and products

Collaborative cybersecurity

Consultation 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?

Strategic approaches to bolstering Australia's security posture should be anchored around collaboration, where no single sector, agency, organisation or individual is wholly responsible for mitigating cyber risks.

Any long-term national strategy needs to be weighed against increasingly organised, well-funded and sophisticated cyber-crime tactics, whether those of Advanced Persistent Threat (APT) groups or rogue scammers. With rapidly accelerating advancements in technology like generative AI, a career in cyber-crime has never been more accessible, especially since larger attack surfaces will continue to be a byproduct of hybrid work and geographically dispersed organisations.

The cumulative result is that there's no limit to malicious actors worldwide, nor is there a limit to their time, resources or targets. Further, they don't need a high success rate to benefit, whereas an organisation only has to fall victim once to suffer irreparable harm. Legitimate organisations' limited resources, combined with the fact that their finance teams are rarely trained cyber experts, mean that Australian professionals face a totally asymmetrical fight.

In other words, no single organisation or individual is equipped to compete in such an imbalanced fight. The most practical and sustainable way forward is through collaborative cybersecurity.

On an organisational level, "collaborative cybersecurity" refers to an approach that sees best-practice security measures, guardrails, and an overarching culture marbled throughout every function, rather than centralised and bottlenecked within information technology (IT) or security teams. It also broadens the umbrella of focus beyond system infiltration and recognises that payments should be guarded as closely as data.

What this means in practical terms is the incorporation of approaches like multi-factor **verification** (MFV), a concept that is distinct from multi-factor authentication (MFA).

Unlike MFA, which uses multiple forms of credentials to establish and authenticate the identity of a user or device, MFV combines centralised and decentralised data from a wide variety of sources to determine the legitimacy of a *piece of information* – for instance, the banking details of a party to a digital transaction. MFV incorporates data sources beyond those originating from within a single system or organisation, leveraging a collaborative network where data can be securely cross-checked against other data.

A separate but related component is what collaboration looks like between businesses. This includes the cultivation of communities or networks in which members can share information confidentially, such as false bank details or known attack tactics. Especially within the context of increasingly asymmetrical cyber challenges, closer collaboration is necessary for tipping the balance back into legitimate organisations' favour.

This is consistent with the Discussion Paper's position that improving and sustaining cyber resilience depends on an "integrated, whole-of-nation endeavour." From a more granular lens, several practicable steps can help achieve this kind of collaborative cybersecurity. Subsequent responses will outline these steps further.

6. How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?

As noted in the Discussion Paper, a recent report found ongoing gaps in agencies' security policies and procedures.[2]

These problems aren't unique to the public sector. According to the AustCyber's Cyber Security Sector Competitiveness Plan, Australians spent $5.6 billion on cybersecurity products and services in 2020.[3] Despite that number, reports of cyber incidents increased by nearly 13% compared to the previous financial year, according to the ACSC.[4]

This consultation acknowledges that correlation does not imply causation, and its intent is not to argue for smaller cybersecurity budgets. However, the figures highlight a noteworthy discrepancy. When considering why cyber-crime reports might be increasing despite significant cybersecurity spending, one factor could be the siloed approaches that often persist throughout both public and private organisations.

For example, an organisation's IT or security department works to prevent threat actors from accessing or breaching its systems and data. However, if an organisation's *supplier* fails to prevent similar breaches, threat actors can more easily weaponise the infiltrated supplier's email account and manipulate the supplier's customers' accounts payable (AP) teams into making fraudulent payments.

These are the sorts of threats that a security team cannot unilaterally prevent. Instead, it's up to financial leaders to ensure organisations' cybersecurity strategies align with their anti-fraud

[2] Australian Cyber Security Centre (2022). *Commonwealth Cyber Security Posture in 2022*. Accessed at www.cyber.gov.au

[3] AustCyber (2022). *Australia's Cyber Security Sector Competitiveness Plan 2022*. Accessed at www.austcyber.com

[4] Australian Cyber Security Centre (2022). *Annual Cyber Threat Report 2021–22*. Accessed at www.cyber.gov.au

financial controls. Organisations must assume that infiltrations and breaches are already happening, if not within their own organisation then within their ecosystem of partners and suppliers.

Across different functions and specialist areas, agencies will need to find strategies and solutions that empower all public servants to mitigate cyber risks and model a more collaborative, integrated approach. This is especially true in functions where popular targets, such as Chief Financial Officers and other C-suite members, are responsible for decisions with major financial or infrastructural consequences.

Collaborative cybersecurity doesn't just include an integrated approach inside the organisation – it also necessitates working closely with external industry partners. Regardless of the partners chosen, agencies can get a better understanding of their unique vulnerabilities and potential solutions by consulting vendors with on-the-ground insights into cyber threats.

Government can bolster these approaches with explicit messaging. When it comes to security, even the most disparate sectors and industries can end up being operationally and financially interdependent. Combined with the asymmetrical advantages of APT groups, this means that no single organisation can guard against cyber threats on its own – this is a message the public sector is well-placed to amplify, especially while emphasising the need for tapping into security-minded networks and communities.

Most crucially, the public sector can lead by example and ensure agencies are deploying best-practice approaches. This includes sharing intra-agency threat information in a secure, private, confidential and formalised way, helping others within the network block threats before an attack can occur.

There is precedence for similar information sharing, with banks routinely sharing risk assessment information with other banks to protect all customers from known fraudulent accounts and other risks. Careful, privacy-minded legislation could compel similar intra-agency sharing of fraud data. If deployed correctly, this would offer a two-fold benefit: it could help the public sector minimise its own vulnerability to common cyber-crime tactics while modelling collaborative cybersecurity for other sectors.

These steps are crucial to ensuring that government can deliver and demonstrate sustainable, effective security practices. They can also help agencies achieve the more preventive, proactive approaches that need to take precedence when designing strategies and systems.

Prioritising prevention

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?

There are several ways that government can support the uptake of cyber security services and technologies in Australia.

The first is similar to modelling collaborative cybersecurity, in that agencies can use their internal strategies and tech stacks to model an emphasis on prevention. At a minimum, this would include a dedicated cybersecurity budget for specific agencies and specialist areas, one that allows the implementation of multiple defence levers.

For example, this typically includes antivirus software, payment protection solutions, intrusion detection, data loss prevention, distributed denial of service (DDoS) protection and firewalls. rather than picking one or two. Every lever should have a demonstrated, clearly understood role and purpose, with budget allocated against each one. Returning to the concept of collaborative cybersecurity, in which security measures are embedded within every function, this budget ideally would not come from a single IT or security team. Instead, these measures would be funded by an overarching budget across the organisation.

Securing larger budgets can be difficult, especially during economic downturns. However, stronger security measures create economies of scale, distributing costs across multiple organisations and bolstering their collective security posture. Collaborative approaches ensure that no single organisation needs to shoulder the full burden of cost.

Furthermore, prioritising cost savings in this area is short-sighted because most incidents risk damage that vastly eclipses any initial savings. Alongside the potential for immeasurable reputational harm and loss of public trust, there are secondary impacts of financial losses that can functionally debilitate organisations, including critical infrastructure providers. Even if they haven't been debilitated directly by ransomware or similar attacks, organisations can still find themselves operationally and financially hamstrung by a loss of revenue, a prolonged inability to repair impacted systems, and knock-on costs such as bringing in external forensic experts.

These risks necessitate a shift toward prevention. While prevention tends to be the goal of most cybersecurity strategies, many of those strategies fail to embed preventive measures throughout the entire organisation. For instance, they might aim to protect critical systems and data, but they don't always include measures for preventing further fallout if a cyber intrusion *does* occur.

This isn't a call for indiscriminate spending. Instead, the right budget can create preventive guardrails throughout the organisation, enabling each agency and function to protect itself against some of the most serious consequences of cyber incidents.

Ideally, those budgets would allow for tools and tactics that facilitate decentralised security approaches and contribute to the security posture of their entire supply chain. They'll also be crucial as organisations take on greater compliance responsibilities around supply chain issues like modern slavery and payment times reporting.

Aside from modelling best practices in prevention, government could consider corporate tax incentives that promote the take-up of these tools, particularly among small-to-medium enterprises (SMEs) with fewer resources and in-house security capabilities. If implemented with the right checks and balances, this might include allowing eligible businesses to claim additional deductions or rebates for specific cybersecurity product spend.

Considering the significant direct and indirect costs of cyber incidents, any budget increases necessary for these incentives are likely to be offset by the prevention of future incidents. Lastly, budget increases should be weighed against the potential for stimulating Australia's technology sector to innovate and export leading-edge security solutions domestically and abroad.

Automating with oversight

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

Best-practice models for automated threat-blocking incorporate two core elements.

The first element recognises the most common attack vector: an organisation's employees. Best-practice models must assume human fallibility while deploying automation to help employees make safer decisions.

The second element relates to data integrity. While automation can mitigate the risk of human error, it should be incorporated into processes with an eye for digital – rather than just analogue – fraud tactics.

For instance, without the appropriate controls or guardrails in place, fraudulent invoice details can make their way into an enterprise resource planning (ERP) system. Because the system can only operate based on the data input rather than cross-matching with external data, it will reinforce erroneous data across multiple processes.

Best-practice automated threat blocking balances these elements, using human-in-the-loop (HITL) principles to limit the fallibility of both human employees and automated systems. As examples, least-privilege access minimises the fallout of human error, while automatic real-time alerts scalably provide information that can help employees avoid making an error in the first place.

One way for government to enhance these measures is to facilitate greater sharing of known attacks and fraud data across the public and private sectors, creating networks that organisations can access in real time and establishing stronger automated defences at scale.

Specifically, broader access to key characteristics of an entity can enable faster, more efficient fraud detection, while minimising the amount of information that needs to be shared. For example, in Australia, Standard Industrial Classification (SIC) codes are only available to government, though this data is more freely accessible in the United Kingdom. Creating similar access to SIC codes in Australia would augment existing measures around automated threat-blocking, and is likely to help individuals and organisations assist in fraud detection.

Eftsure is grateful to the Department of Home Affairs for the opportunity to contribute to a productive discussion on the 2023-2030 Cyber Security Strategy. Should the Government wish to further explore any points raised in this submission, Eftsure would be pleased to cooperate.

Kind regards,

[redacted]

Mark Chazan
Chief Executive Officer
eftsure Pty Ltd
eftsure.com.au
1300 985 976