Strengthening Australia's Cyber Security Regulations and Incentives

Submission to the Discussion Paper

FINAL

1. Executive Summary

Thank you for the opportunity for Okta to contribute to this critical area of government policy.

Okta, like the Australian Government, views cyber security as a shared responsibility between governments, businesses and the community.

Okta's assessment of the current threat landscape broadly aligns with observations published in the discussion paper. Okta's technology is designed to limit the effectiveness of the credential-based attacks that the ACSC identifies as the root cause for the majority of incidents it responds to.

The Government's discussion paper was a refreshing read. Its authors demonstrate a solid grasp of the root causes of cyber security incidents, and the need for careful examination of potential policy solutions to ensure they are effective, on the one hand, and limit unintended consequences on the other.

If any of the feedback provided below requires further explanation, please contact:

Brett Winterford
Senior Director, Cybersecurity Strategy
Okta
[redacted]

About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organisations to securely connect the right people to the right technologies at the right time. With over 7,000 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely use the best technologies for their business. More than 10,000 organisations, including JetBlue, Nordstrom, Slack, T-Mobile, Takeda, Teach for America and Twilio, trust Okta to help protect the identities of their workforces and customers.

Responses to the discussion paper

1. What are the factors preventing the adoption of cyber security best practice in Australia?

Okta broadly concurs with characterisation of market failures in the discussion paper that hamper the ability of security teams to prevent, detect and respond to cyber security events.

2. Do negative externalities and information asymmetries create a need for Government action on cyber security? Why or why not?

Given the threat environment and the costs incurred by victims of cybercrime, it is appropriate that the Australian Government continually assess what action it might need to take to protect Australians from harm.

Okta commends the authors' approach to assessing the potential impacts and costs of policy proposals, underpinned by a solid set of best practice principles listed in Appendix B of the discussion paper.

Imposing new obligations on end-user entities can, in some circumstances, burden those entities with managing complex risks they have little to no control over. This is especially acute for SMEs that have little leverage to negotiate for access to security features bundled as premium services by dominant technology suppliers. The discussion paper provides a sufficient number of policy alternatives to avoid these scenarios.

3. What are the strengths and limitations of Australia's current regulatory framework for cyber security?

Australia's regulatory environment is, by global standards, well-balanced in terms of the interests of all stakeholders. Regulation tends to be reserved for addressing the negative externalities of events that cause the most harm to individuals.

Outside of consumer protection and privacy laws, regulation of cyber security in Australia is largely sector-specific. The discussion paper observes that there are circumstances where protections are absent or where regulators overlap.

For example, Australian Consumer Law provides recourse for individuals victimised by payments fraud[1]. But the same protections aren't always available to small businesses.

[1] ePayments Code, ASIC

This is particularly problematic for SMEs that suffer losses from Business Email Compromise events. Reducing exposure to this category of fraud requires action on multiple fronts: stronger default settings by providers of email services on the one hand, by banks on the other, as well as improved security hygiene among targeted organisations.

Unfortunately, there has been little progress during the seven years that this category of fraud has grown exponentially[2]. Arguably, the problem won't be addressed while financial services and technology services are regulated under different regimes.

4. How could Australia's current regulatory environment evolve to improve clarity, coverage and enforcement of cyber security requirements?

The discussion paper puts forward a range of commendable suggestions, which we've discussed in specific answers below. We have added two further suggestions in the answer to question 28.

5. What is the best approach to strengthening corporate governance of cyber security risk? Why?

In our view, the role of the board in governing an organisation's cyber security posture is to:

- Determine the organisation's risk appetite as it applies to cyber loss events; and routinely assess whether the organisation is operating within the bounds of acceptable risk;
- Appoint and document the role of an appropriate committee to provide oversight of cyber risks;
- Ensure management has clearly defined the ownership and accountability for managing cyber risks;
- Continually benchmark the maturity of the organisation's cyber security capabilities against customer expectations, regulatory and other legal requirements and industry peers. This is best measured by engaging third parties to independently audit these capabilities against recognised risk management frameworks, such as the NIST Cybersecurity Framework[3].
- Receive regular updates from management regarding cyber risk management and incident response preparedness, ensuring that sufficient resources are being provided to remediate gaps.

It would be advantageous to all stakeholders for these responsibilities to be codified and communicated by a professional body. We agree that the set of principles[4] laid out by the ASX Corporate Governance Council presents an appropriate model to consider.

[2] Internet Crime Complaint Center, April 2020

[3] NIST Cybersecurity Framework

[4] Principles and Recommendations, ASX Corporate Governance Council, February 2019

We have observed that even in organisations where these responsibilities are well-understood, there is a need for more explicit guidelines, ideally set by an impartial body and subject to regular review.

In many listed organisations, board discussions about cyber security are limited to a 30-minute slot in the quarterly board audit committee meeting. Until recently, this has been considered best practice. The audit committee meeting is a forum in which cyber security issues compete for mindshare among a range of other risks (financial risks, active litigation, breaches of company policy etc) that tend to be more immediately understood by long standing directors. So at times, cyber security is treated as a bit of an afterthought.

Progressive organisations are now appointing dedicated subcommittees for governance of cyber security risks. This allocates at least 90 minutes a quarter (vs 30) to what is a nuanced and complex area of risk management.

It is Okta's view that governance standards should only become mandatory (Option 2 in the discussion paper) if voluntary standards fail to shape better security outcomes.

6. What cyber security support, if any, should be provided to directors of small and medium companies?

Okta recognises that small businesses are the parties most vulnerable to disruption and loss from cybercrime in the Australian economy.

In most areas of cybercrime, small businesses are targeted as often as large organisations. But small businesses are far less resilient to security incidents. Prior to the COVID-19 pandemic, US survey data[5] revealed that one in four small businesses that suffered a data breach would later file for bankruptcy, while one in ten went out of business permanently.

COVID-19 exacerbated the problem. Stay-at-home orders in 2020 forced many small businesses to open up remote access to internal systems[6] for the first time, often in the absence of the infrastructure or skills to do so securely. This resulted in a spate of at-scale, opportunistic attacks on organisations that failed to securely configure remote access.

These attacks also revealed a pattern of underinvestment in several categories of on-premise network and endpoint security products that had typically been sold into small and medium-sized businesses. As more small businesses recognise the security benefits of consuming applications as-a-service, established vendors have either failed to adequately maintain these products or walked away from the small business market altogether[7].

[5] National Cyber Security Alliance, 2019
[6] Cyber Readiness Institute, April 2020
[7] EOL notice for Symantec Small Business Edition, Broadcom, February 2020

Exacerbating this problem, SMEs are typically unable to afford to invest in vulnerability management. In 2020, over 18,000 vulnerabilities were reported to the public (assigned CVEs). Over half of them (10,000) were rated high or critical. Few if any SMEs have the skills, resources or motivation to address these vulnerabilities. Effective vulnerability management requires that out-of-cycle patches -- which are often prone to being ineffective or the cause of system downtime -- are extensively tested by end user organisations prior to being installed. This testing requires infrastructure and skilled resources that many small businesses do not have available.

The scale of this problem is imposing and presents a quandary for the policy community. It's also a problem the broader community can't afford to ignore. The digital assets of small businesses are often viewed by threat actors as soft targets that can be exploited for use as jumping off points in larger campaigns.

Okta views this problem in the context of a shared responsibility between all stakeholders in Australia's digital ecosystem.

One way to tackle a problem of this scale is to borrow from the adversary's tradecraft. There are numerous passive, legal tools cyber security professionals use to discover when organisations are exposed to high severity vulnerabilities in internet-facing infrastructure.

The authors of this document were involved in the creation of the CTI League, a volunteer organisation that disclosed and coordinated responses to several thousand exposed devices in medical facilities over the first year of the COVID-19 pandemic[8]. If the CTI League's experience is any indicator, there are a large number of trusted, motivated individuals in the information security sector who could be potentially tapped to assist the ACSC in applying the same service to small businesses in Australia. Indeed, many of the industry's top professionals were trained by the ASD, but have since been recruited into highly-paid roles in industry. They haven't necessarily lost their sense of mission.

To be successful, an undertaking of this kind needs to be led by an independent, respected party (such as the ACSC), which would prioritise scanning activities and set appropriate scope.

Government assistance may also be required when volunteers need to identify a relevant security stakeholder from affected businesses. This is no small undertaking: in most circumstances, an SME doesn't have staff trained to handle security issues. But they should nonetheless be obliged to simply put forward a person to receive notifications about vulnerabilities in their systems when those flaws are externally observable. (To use a transport analogy: when your car is found to be unsafe you get a "fix it ticket". No-one expects you to be a mechanic, but they do expect you to go to a mechanic and get it fixed.)

In the United States, lawmakers are in the process of drafting bills that may require all organisations to put such a candidate forward. Australia should consider a similar approach.

[8] CTI League Report, March 2020 [pdf]

Okta's Security team would be happy to work with policymakers or the ACSC to help stand up a program.

In the longer term, the government should also consider how to provide tools that help SMEs measure their own cybersecurity hygiene. We would endorse programs that attempt to make the ACSC's advice and guidelines more digestible and actionable for small businesses.

The UK NCSC has made interactive tools available that help SMEs assess their cyber security exposure (the "early warning[9]", "mail check[10]" and "web check[11]" services). These services are relatively easy to build, as many aspects of an organisation's cyber hygiene are externally observable.

The larger challenge is one of ongoing funding: these tools require active maintenance by dedicated teams if they are to remain relevant over time. This is an area where government leadership and investment would pay dividends across the economy.

7. Are additional education and awareness raising initiatives for senior business leaders required? What should this look like?

Okta encourages the Australian Government to revisit its 2017 Cyber Health Check[12], which surveyed ASX100 directors to gauge the level of awareness of cyber security risks and the plans in place to address them.

Anecdotally, we have observed that the Australian business community has made considerable progress in recognising cyber-related risks, thanks largely to the initiatives set in motion by the 2016 Cyber Security Strategy. But this observation needs to be tested.

There is some cause for optimism. Okta has observed a surge in demand for single sign-on (SSO), multi-factor authentication and passwordless solutions. These technologies herald a future where the primary categories of incidents (credential phishing, for example) identified in this discussion paper might be significantly reduced. According to a 2021 study commissioned by Okta[13], a larger number of organisations in our region are also exploring modern "zero trust" architectures that aim to address the problem of implicit trust that is so often abused by ransomware actors.

[9] Early Warning service, NCSC
[10] Mail Check service, NCSC
[11] Web Check, NCSC
[12] ASX 100 Cyber Health Check Report, Australian Stock Exchange, April 2017
[13] The State of Zero Trust Security in Asia Pacific, Okta, 2021

8. Would a cyber security code under the Privacy Act be an effective way to promote the uptake of cyber security standards in Australia? If not, what other approach could be taken?

Okta does not have a fixed position on which legislative instruments are the most appropriate for promoting the uptake of cyber security standards.

That being said, Australia's Privacy Act offers a framework for limiting the scope of this proposed security code. It would narrow the scope to those externalities associated with the breach of personal information and only be applicable to organisations that could feasibly afford to comply (those with revenues over AU$3m).

A larger area of concern is whether the Office of the Australian Information Commissioner is provided the funding or talent to enforce a code[14], or whether a separate, dedicated body is required.

9. What cost effective and achievable technical controls could be included as part of a code under the Privacy Act (including any specific standards)?

We are pleased to see the Government approach the introducing minimum technical standards for the protection of personal information.

The widespread adoption of the priority controls (encryption of data in transit and at rest, strong passwords, multi-factor authentication and timely application of critical patches) listed in the discussion paper would go a long way to protecting the personal information of Australians.

Of these priority controls, multi-factor authentication is one of the simplest and most powerful protection against a variety of threats. An economy-wide requirement to use multi-factor authentication for access to PII data would inhibit a huge range of attacks, with relatively low implementation costs.

We also agree that the proposed code would need to keep pace with changes in the threat environment and innovation in the control environment[15].

[14] Weak, Dysfunctional Privacy Office Needs More Money - InnovationAus, February 2021

[15] To illustrate: no two authentication factors have the same security properties. Okta's identity platform supports the broadest range of factor types, and administrators can write policies in which the factors required are applied according to real-time user, device or network context, as well as the criticality of the resource (apps or data) the user is attempting to request. New customers are embracing passwordless access ('Okta FastPass'), underpinned by a smaller number of high assurance factors such as cryptographic relationships between the user device and the identity cloud, biometrics and other phishing-resistant factors.

We also concur with the government's assessment that the Essential 8, for all its many merits[16], is not the appropriate vehicle for a cyber security code under the Privacy Act. The scope of the Essential 8 is limited to protection of Windows-based, internet-connected networks. It lacks direct applicability to the protection of citizen data in modern, cloud-based environments[17].

10. What technologies, sectors or types of data should be covered by a code under the Privacy Act to achieve the best cyber security outcomes?

Okta recommends keeping the scope of such a code as straightforward as possible to ensure it is well understood by industry. For example, it might only apply to access to PII data (authentication) and storage (encryption) of PII data by any entity caught by Australia's Privacy Act. It should be technology and sector agnostic.

11. What is the best approach to strengthening the cyber security of smart devices in Australia? Why?

The majority of manufacturers of smart devices used in Australia are not domiciled in Australia. We are not confident that manufacturers will have enough commercial incentive to introduce security features or change security practices until a significant number of jurisdictions harmonise on minimum standards.

Fortunately for Australia, some of our key allies have already coalesced around the same standard (ESTI EN 303 645[18]) as a basis for minimum standards in smart devices.

This presents an opportunity for action.

12. Would ESTI EN 303 645 be an appropriate international standard for Australia to adopt as a standard for smart devices? If yes, should only the top 3 requirements be mandated, or is a higher standard of security appropriate?

Yes. ESTI EN 303 645 is both comprehensive and the foundational document for regulations in multiple jurisdictions that have the same concern for consumer protection as Australia.

The top three requirements in the standard would make for an excellent foundation upon which the remainder should progressively be introduced.

[16] The ACSC Essential Eight: Delivering MFA for all Australians, July 2021
[17] Okta nonetheless endorses the close alignment between the Essential 8 Maturity Model and the NIST 800-63B standard, which demands the use of higher assurance factors according to an assessment of risk.
[18] Cyber Security for Consumer Internet of Things: Baseline Requirements, ETSI, June 2020

13. Would you be willing to voluntarily remove smart products from your marketplace that do not comply with a security standard?

N/A to Okta.

14. What would the costs of a mandatory standard for smart devices be for consumers, manufacturers, retailers, wholesalers and online marketplaces? Are they different from the international data presented in this paper?

N/A to Okta.

15. Is a standard for smart devices likely to have unintended consequences on the Australian market? Are they different from the international data presented in this paper?

N/A to Okta.

16. What is the best approach to encouraging consumers to purchase secure smart devices? Why?

Manufacturers that have prioritised security in the absence of regulation deserve to be rewarded for their efforts in the short-term, prior to the introduction of laws that mandate minimum standards.

The voluntary labelling scheme pioneered in Singapore[19] provided incentives for manufacturers to differentiate themselves on security. This promotes an environment in which manufacturers, retailers and service providers, technology media and social media have an incentive to amplify positive security messages in their communities, setting new expectations among consumers.

Longer term, these expectations need to be codified in law.

17. Would a combination of labelling and standards for smart devices be a practical and effective approach? Why or why not?

If adequately resourced and sequenced, the schemes could complement each other: with minimum labelling preceding minimum standards.

Manufacturers should also be given indicative timelines for when more stringent requirements will be added to either scheme, such that the government incentivises and rewards those that

[19] Cybersecurity Labelling Scheme, CSA Singapore

invest in secure-by-design programs from the outset.

18. Is there likely to be sufficient industry uptake of a voluntary label for smart devices? Why or why not?

Okta has insufficient data to confidently answer this question.

19. Would a security expiry date label be most appropriate for a mandatory labelling scheme for smart devices? Why or why not?

This idea has a great deal of merit. Ultimately, the security of a device is intrinsically tied to the level of support the manufacturer commits to it.

20. Should a mandatory labelling scheme cover mobile phones, as well as other smart devices? Why or why not?

Any device with a rapid refresh cadence -- mobile devices included -- would benefit from clearly defined parameters. Currently there are a large number of mobile devices that get indeterminate or unpredictable levels of support almost as soon as they launch. Clarifying this would be beneficial to all stakeholders.

21. Would it be beneficial for manufacturers to label smart devices both digitally and physically? Why or why not?

Yes. While physical labels may provide appropriate guidance prior to purchase, labels applied digitally (i.e. on the manufacturer's web site or in the management interface of the device) would serve to help consumers keep track of these commitments during the life of the product.

22. Would voluntary guidance encourage Australian businesses to implement responsible disclosure policies? If not, what alternative approaches should be considered?

Yes. This is an example of where the government can and should lead by example.

In the United States, the Cybersecurity and Infrastructure Security Agency (CISA) published high quality advice, templates and other resources[20] on vulnerability disclosure policies prior to making them mandatory for all US government agencies.

Those resources were eagerly consumed by private sector entities. More importantly, CISA's advocacy helped to validate the practice in the private sector.

[20] Improving Vulnerability Disclosure Together, CISA, September 2020

23. Would a cyber security health check program improve Australia's cyber security? If not, what other approach could be taken to improve supply chain management for small businesses?

There is a potential that a program of this scale would stretch the limited resources of the ACSC, without much guarantee of success.

There are simply too many variables that are difficult to test at a national scale.

There are a variety of "scorecard tools" that rank the security of an organisation according to externally observable indicators in its domain. These tools are typically used for self-diagnosis or for third-party security governance (i.e. as a proxy for an in-depth assessment of a company's maturity).

Many of the "scorecard" tools lack crucial context about the organisation and very often generate false positives. They do not provide the scope necessary for a trust mark to be meaningful. As the discussion paper observes, trust marks can (and historically have) given consumers a false sense of security.

A more effective strategy would simply be to require small businesses to identify a person to receive notifications about externally-visible vulnerabilities in their systems.

24. Would small businesses benefit commercially from a health check program? How else could we encourage small businesses to participate in a health check program?

See answer to question 23.

25. Is there anything else we should consider in the design of a health check program?

See answer to question 23.

26. What issues have arisen to demonstrate any gaps in the Australian Consumer Law in terms of its application to digital products and cyber security risk?

Okta has no comment on potential gaps in Australian Consumer law.

27. Are the reforms already being considered to protect consumers online through the Privacy Act 1988 and the Australian Consumer Law sufficient for cyber security? What other action should the Government consider, if any?

See answer to question 26.

28. What other policies should we consider to set clear minimum cyber security expectations, increase transparency and disclosure, and protect the rights of consumers?

The Australian Government may wish to add two more ideas to the many commendable proposals put forward to address these issues.

The first is the use of government purchasing power to incentivise better security practices across the technology ecosystem.

In the United States, the Biden Administration's May 2021 Executive Order on Improving the Nation's Cybersecurity[21] recognises that "the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security."

The EO decrees that "the Federal Government must lead by example" by setting more stringent standards and requirements for cybersecurity for government agencies. This harnesses the enormous buying power of US government agencies to demand stronger default settings from technology suppliers. For example, the administration is setting policies[22] that aim to convince cloud service providers to restore the provision of audit logs as a default feature[23] (rather than a premium service[24]).

US Government agencies were also asked to implement multifactor authentication, endpoint detection and response and data encryption universally, and asked to plan a transition from the pervasive model of domain trust to a zero trust model for access to systems.

When the Australian Government demands a higher standard for the security of the cloud services it consumes, those same capabilities are by consequence more available to Australia's private sector.

The second idea relates to director liability and corporate governance of cyber security. As previously stated, the discussion paper articulates the trade-off between the benefits and costs of inaction, voluntary governance standards and mandatory standards. The government's best practice principles demand that any new regulation must consider unintended consequences.

[21] Executive Order on Improving the Nation's Cybersecurity, The White House, May 2021
[22] Improving the Federal Government's Investigative and Remediative Capabilities, OMB, August 2021
[23] Capturing High Value Audit Events, *Office365ITPros*, March 2020
[24] Addressing Audit Log Storage for US Federal Government Customers, Microsoft, April 2021

Okta recommends the policy community be mindful of how the path chosen might influence the security culture of affected organisations. When security events are handled in secrecy, affected organisations are less able to learn from their mistakes, let alone educate industry peers or the broader community. This allows adversaries more time and space to apply the same tradecraft against more victims and impose further costs on the community.

One of the worst possible outcomes from the introduction of more prescriptive standards would be scenarios in which:

- Directors that lack confidence in the organisation's security program are anxious about the additional liabilities they might be exposed to if the organisation is transparent about security events; and
- Executives and staff are subsequently encouraged to conceal security events or avoid candid conversations about cyber security.

While it is outside the scope of this paper, the Australian Government should consider what protections, within reasonable limits, might be afforded to organisations that are proactively transparent about security events. Some form of protection might be applicable to events where directors dutifully met the expectations set under voluntary governance standards, and the executive took earnest efforts to prioritise and treat cyber-related risks, but the organisation was nonetheless unable to prevent a compromise event. Further protections might be offered to organisations that publish post-incident reports, written to government-decreed specifications, that detail precisely how the adversary achieved their goals.

Organisations cannot expect to be afforded protection from all adverse effects of security incidents, but should be protected against the specific consequences of coming forward to voluntarily disclose information about an incident.

This is an evolving area of policy[25] that is largely untested. But in our view, an exploration of corporate governance for cyber security needs to also consider how best to facilitate the "no-fault reporting" of cyber security incidents for balance.

[25] Finally! A Cybersecurity Safety Review Board - *Lawfare*, June 2021