kaspersky

Comments Regarding Strengthening Australia's Cyber Security Regulations and Incentives

Kaspersky's Submission
August 2021

We at Kaspersky applaud the efforts of the Australian government to enhance the cybersecurity of a growing digital economy in Australia through incentivizing businesses to invest more in digital security. These issues are currently being discussed in other jurisdictions as well as within the Organization for Economic Co-operation and Development (OECD), where Kaspersky is listed among contributors to its 2021 reports on 'Enhancing the digital security of products'[1] and 'Encouraging vulnerability treatment'[2]. These topics and solutions for tackling information asymmetries and negative externalities are also being discussed within the multistakeholder forums such as the Paris Call for Trust and Security and its Working Group 6, co-chaired by Kaspersky and Cigref, as well as within the Geneva Dialogue[3] – an international conversation led by the Swiss Federal Department for Foreign Affairs (FDFA) and implemented by DiploFoundation.

All of this allows us to navigate through these issues while constantly interacting with different regulators and industry partners, including small-and-medium enterprises (SMEs), and, therefore, share our perspective below to the questions outlined in the public consultation.
We hope our input to some of the questions could be helpful, and once again we firmly support the intentions and further plans of the Australian government to build a cyber-secure and cyber-resilient digital economy while also protecting users of ICT products and services.

What are the factors preventing the adoption of cybersecurity best practices in Australia?

This is a common problem, which is not unique to Australia. Businesses in Australia, including owners and operators of critical infrastructure entities, are not always fully aware of the risk they inherit, the risk they own, the risk they pass on, and the risk they bear for economic security as well as the security and safety of users. In most cases our interaction with enterprises, including SMEs in Australia and abroad, allows us to see that individual business risks are not aligned with and do not include cybersecurity risks. Most businesses are learning more and more about cybersecurity incidents and major hacks taking place elsewhere; however, few of them see cybersecurity risks as relevant in their country or to their businesses. Broadly speaking, people do not understand the 'permeability' of cybersecurity risks and cybercriminal activities, which can impact them in a real way, at any time. Even if they do – many of them do not have knowledge of what can and should be done for cybersecurity protection. The lack of funding for cybersecurity, particularly in the SME sector, is another important factor.

In addition to this, businesses lack financial incentives for better cybersecurity behaviour, which could be partially tackled through stimulating a vibrant insurance market. Existing standards and security practices remain largely voluntary, with little awareness raising efforts for businesses to learn about them and understand which of them should be applied and how, considering the scope and size of their business operations. This also highlights the urgent necessity of the

[1] https://www.oecd-ilibrary.org/science-and-technology/enhancing-the-digital-security-of-products_cd9f9ebc-en
[2] https://www.oecd-ilibrary.org/science-and-technology/encouraging-vulnerability-treatment_0e2615ba-en
[3] https://genevadialogue.ch/

education piece to help businesses to see the benefits of aligning cybersecurity risks with their operational business risks to be more effective and competitive on the market.

Usually, the State would play a more proactive role in this education process in some of the more developed countries such as Singapore within the Asia-Pacific region. However, for most countries, there appears to be room for deeper understanding of how the State can play this role effectively through public-private partnerships and through regional cooperation, and to educate its local businesses and people for greater cyber maturity across the board.

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

Yes, they do. Companies' decision-making regarding investment choices is influenced by the return on investment (ROI); thus, the chief executive officer (CEO) of a medium-sized company would likely ask: 'Why do I need to think about making my products safer? How would it profit me to innovate further?' Instead, that typical CEO would likely decide 'to optimize production and product-support costs; come up with new, attractive features; and have consumers change products faster'.

The role of the government, in this case, seems critical: in consultation with the private sector, the government needs to create the right economic environment as well as to help SMEs, which often lack resources and capacity, with certain targeted policy tools that would be part of the common technology ecosystem. In building closer dialogues and trusted partnerships with companies of any size, the government's role is to shape the rules so that cybersecurity becomes a competitive advantage. Addressing the lack of resources and capacity through stimulating educational programmes and research and investment (R&D) is another possible direction in which the government can play a critical role.

The second reason for greater government intervention for building a cyber-resilient digital transformation is the existing complexity of regulatory approaches. At the SAP Product Security Summit in 2019, Holger Mack and Tom Schröer showed that in today's IT products, less than 5% of the computer code is home-grown; the rest is code of third-party companies or third-party components. Why is this so?

To produce and deliver faster, as well as to ensure the interoperability of IT products, businesses need to optimize their software development and use modules of other vendors. However, growing in complexity and sophistication, modern software products are becoming more vulnerable. In managing modern IT products, into which a great many third-party components are embedded, the manufacturer needs to decide: (1) which certification is necessary to pass, and (2) how certification should be approached. The answer to both questions may not satisfy the needs because there is no institutional framework in which certification could be considered optimal within the Australian market. What is more, it is impossible to imagine stand-alone certification for the entire technology stack: for each module and component, there would be, probably, separate certification requirements. While large enterprises are more likely to be able to handle this, SMEs would face a huge burden to their business, in terms of resources and know-how, in attempting to ensure rigorous regulatory compliance.

For businesses that do not produce software but rely on it, including for data processing, the same question would arise: what controls and practical steps, as based on the existing regulatory frameworks and laws in Australia, should be implemented for optimal cybersecurity and

compliance? Answering this would greatly simplify the cybersecurity risk-mitigation strategies for businesses.

Therefore, again, the government, in consultation with the private sector, which comprises not just local enterprises but foreign multinational companies, needs to address this issue by agreeing on baseline security requirements and on different layers of certification to address different levels of the criticality of technologies. The idea behind this is to secure technology and enhance confidence in technology through standards and certification – but this has to be made proportionate to the companies' size and sector of operations.

What are the strengths and limitations of Australia's current regulatory framework for cyber security? How could Australia's current regulatory environment evolve to improve clarity, coverage and enforcement of cyber security requirements?

Australia currently has a rather limited cybersecurity regulatory framework. Certain industries, such as financial services and the energy sector, are aligned to global standards such as the CPS234 standard, which requires all financial services to have an appropriately sized information security capability, systematically test the security, notify APRA of incidents, and define the cybersecurity roles of board members and management within the business. The energy sector has the Australian Energy Sector Cyber Security Framework (AESCSF), which has been developed through collaboration with industry and government stakeholders, including the Australian Energy Market Operator (AEMO), Australian Cyber Security Centre (ACSC), Critical Infrastructure Centre (CIC), and the Cyber Security Industry Working Group (CSIWG), which includes representatives from Australian energy organizations. The AESCSF leverages recognized industry frameworks such as the US Department of Energy's Cybersecurity Capability Maturity Model (ES-C2M2) and the NIST Cyber Security Framework (CSF), and references global best-practice control standards (e.g., ISO/IEC 27001, NIST SP 800-53, COBIT, etc.). The AESCSF also incorporates Australian-specific control references, such as the ACSC Essential 8 Strategies to Mitigate Cyber Security Incidents, the Australian Privacy Principles, and the Notifiable Data Breaches scheme (NDB).

The first version of the Critical Infrastructure Act 2018 was silent on cybersecurity. However, it is hoped that the updated law will mandate the adoption of the ACSC Essential 8 Strategies to Mitigate Cyber Security Incidents.

Lastly, any Australian organisation that experiences a data breach where personal information is accessed, disclosed without authorization, or lost, must report this to the Office of the Australian Information Commissioner under the current Notifiable Data Breach Act (revised in 2017).
This brief overview indicates the ongoing legislative efforts to incorporate cybersecurity protections and mindset into the broader regulatory landscape in Australia. However, our observation shows that currently Australia has a set of complex regulatory pieces rather than a stand-alone harmonized institutional landscape, which creates a difficulty for businesses to navigate through this and identify all necessary pieces they have to be aware of.
In addition, the existing legislative frameworks do not always provide clarity on liability in case known and unpatched vulnerabilities are exploited and lead to cybersecurity incidents. Timely patch implementation on the code/system owner (vendor) side is not always incentivized, which creates frustration for security researchers to act responsibly for coordinated vulnerability disclosure and leads to security and safety risks for users.

Separately, the market for cyber insurance continues to fail to deliver on this full potential. Quite often insurers struggle to find underwriters and claims adjusters; however, where cyber experts

exist, insurers apply insufficient or inconsistent models for evaluating cyber risks. As a result, insurers remain hesitant to assume meaningful amounts of risk that would define a healthy cyber insurance market.

Supply chain risk management is another area requiring improvements. Practically, as Australian businesses participate in the global marketplace, it is important that they have sufficient means and knowledge to identify and assess their critical dependencies (including components and materials). In this regard, the existing legislative framework needs to introduce further funding and capacity building efforts to support businesses in securing their IT systems and networks, and thus securing the economy and society in Australia. As an example, Kaspersky offers the Cyber Capacity Building Program[4] – a dedicated training to provide security evaluation knowledge to businesses, government organizations and academic institutions for assessing their supply-chain cyber-resilience.

Therefore, to sum up, the following improvements could be considered for a clearer and more efficient regulatory environment:

- developing baseline security requirements for businesses to make sure they are interoperable and proportionate to the scope, size and scale of their business operations (practically, businesses need to know what the optimal level of security is and how, in an ongoing effort, it can be achieved). This would also require further funding, education and capacity building efforts.
- mandating ongoing cybersecurity evaluations/audits – from baselines to the most advanced depending on the size, scope and scale of businesses' operations.
- creating education efforts to users of ICT products and services to make sure they are sufficiently informed about their liability and duty of care in using ICTs. Further investments in cyber-education of users will trigger more user requests for quality and reliability of ICT products and services. While this could be considered as a negative cost-added factor for businesses, it is important to realize that security-conscious user behaviour leads to security conscious behaviour on the side of manufacturers of ICTs and businesses overall (as they would continue to compete on the market where security would now be considered as an important feature/offer for users).
- developing a robust and functioning market for insurance products through: claims adjuster training and certification; underwriter training and certification; developing frameworks and research methodologies for understanding and accurately pricing cyber risks; and identifying common areas of interest for donating and pooling anonymized data that can be used for more accurate risk models.
- encouraging further responsible vulnerability management and disclosure processes, including through incentivizing timely patch implementation (e.g., developing guidance, placing a cap on insurance payouts, or creating liability for incidents that involve unpatched systems), incentivizing responsible vulnerability research/analysis and disclosure (e.g., creating programs of cooperation between vendors and security researchers), educating businesses on the necessity of CVD policies and processes.
- developing voluntary certification and labelling schemes for cybersecurity products with several layers of risk attestation (from baseline to the most advanced) to enhance user trust in ICTs as well as equip users with sufficient information about the functioning and security of ICTs before purchases.

[4] https://media.kaspersky.com/en/cyber-capacity-building.pdf

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

In addition to the input above, we see a need to develop a framework with mandatory baseline best practices for businesses, where further layers of cybersecurity protections and steps are added in a voluntary way to enhance businesses' competitive advantage.

In other words, a base level is mandated for businesses, where other specific industry-relevant layers of cybersecurity protections and mitigations are additional options, catering to businesses pursuing greater excellence in managing cyber security risks.

We believe this – working as a 'Lego' or building-block approach – would be most effective by enabling compliance in a structured manner and reducing cybersecurity risks. And if the State deems fit, government incentives can be introduced to encourage more to pursue best practices, through policy tools such as introduction of a quality mark or certification of approval to set apart businesses with truly robust cyber security best practices.

What cybersecurity support, if any, should be provided to directors of small and medium companies?

In line with our above-mentioned feedback, for small to medium companies, cybersecurity awareness is key for directors to understand the risks, how threat actors target their businesses, how these attacks can impact their business, and how to mitigate these risks.

In this regard, it is crucial to create cybersecurity awareness and education programs to provide capacity-building resources to SMEs.

A complementary approach could be the 'carrot rather than stick' approach, where businesses are incentivized to adopt cybersecurity measures for clear and tangible benefits. For instance, the UK government used a cashback scheme offering payments to households who use solar technology, which helped increase the amount of green energy and facilitate households' move over to low-carbon energy. Perhaps something similar could be adopted for creating financial benefits and incentives to businesses, including SMEs.

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

We do not think that additional initiatives should be created. Rather, we need an ongoing drip-feed approach to continually educate business leaders of the evolving cybersecurity risks and how best to address them. It is important to continue repeating the same messages consistently so that over time they become the norm.

And beyond getting the messages through, they would need concrete and actionable items to push through the necessary implementation beginning from within their own organisations, and the determination to see them through.

Would a cybersecurity code under the Privacy Act be an effective way to promote the uptake of cybersecurity standards in Australia? If not, what other approach could be taken? What cost effective and achievable technical controls could be included as part of a code under the Privacy Act (including any specific standards)?

Yes, we would agree that a cybersecurity code under the Privacy Act could be an effective way to promote the uptake of cybersecurity standards in Australia. We believe a cybersecurity code needs to serve as guidance to organizations on organizational and technical steps to achieve data protection by design and by default – concepts specifying cybersecurity measures for the protection of personal information. It is important to model the code minding several levels of risk appetite and attestation that would help businesses apply the optimal amount of measures proportionate to their size and scale of operations on the market.

With regard to particular technical controls, we would recommend those that allow organizations to implement data protection principles: transparency, lawfulness, fairness, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability. We at Kaspersky have previously shared the feedback[5] on particular controls to the Guidance by the European Data Protection Board (EDPB)[6], and believe that a similar approach could be borrowed for developing the cybersecurity code in consultation with industry and privacy experts. The Guidance lists key design and default elements to implement each principle mentioned above.

What is the best approach to strengthening the cybersecurity of smart devices in Australia? Why? What is the best approach to encouraging consumers to purchase secure smart devices? Why? Would a combination of labelling and standards for smart devices be a practical and effective approach? Why or why not? Voluntary star rating (Option 1)

The approach to strengthening the cybersecurity of smart devices in Australia needs to include a complex set of the following steps:

- adoption of a voluntary star-rating certification and labelling scheme, with several tiers of risk attestation (thus we support option 1, i.e., a combination of labelling and standards). For IoT/smart devices applied in critical infrastructure, higher security risk attestations should be required. Similar efforts have been implemented in Singapore through the Cybersecurity Labelling Scheme with four (4) different tiers of assessment – from baseline requirements to penetration testing. Labels based on certification would help consumers to make informed purchase decisions based on the security provisions of the smart devices.
- development of policy actions tackling the end-of-life (EOL) gap, i.e., the stage of the product's lifecycle when supply-side actors cease to support the product and issue security updates. Once this is misaligned with the end-of-use (i.e., the stage when end-users cease to use the product), this creates a security and safety risk to consumers of IoT/smart devices. These policy actions could include actions on requiring supply-side actors to design and implement clear and transparent EOL policies for their products and publicly state the minimum length of time for which a product will have security updates. It could be equally important to incentivize consumers to stop using a product when it reaches the EOL through informing them about potential cybersecurity risks.

Would ESTI EN 303 645 be an appropriate international standard for Australia to adopt as a standard for smart devices? a. If yes, should only the top 3 requirements be mandated, or is a higher standard of security appropriate? b. If not, what standard should be considered?

[5] https://www.kaspersky.com/about/policy-blog/index/guidelines-on-data-protection-by-design-and-by-default
[6] https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

kaspersky

Overall, ETSI EN 303 645 seems to be an appropriate international standard, though some guidelines are needed to specify the interpretation of some provisions and examples/use cases where these provisions can be most effectively applied. Unfortunately, in certain cases the standards make the provisions insufficiently specific (e.g., in provision 5.1-3, when it comes to authentication mechanisms, it is not clear what cryptographic algorithms should be used).

The implementation of mandatory requirements needs to be done depending on the particular risk tier (from baseline to the most advanced), but in principle we agree that the top three requirements – no default passwords, implementing a vulnerability disclosure policy, and keeping software updated – seem to be foundational and need to be mandated as basics.

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

The voluntary guidance is crucial to support Australian businesses in implementing responsible disclosure policies. The guidance needs to include the following elements:

- providing information on steps in establishing policies for vulnerability management and disclosure (e.g., based on the 2021 OECD report on 'Encouraging vulnerability treatment: Overview for policy makers'[7]), as well as support in behaving ethically and responsibly. E.g., Kaspersky published its Ethical Principles for Responsible Vulnerability Disclosure, inspired by the FIRST Code of Ethics. Our Ethical Principles provide greater transparency in vulnerability handling by Kaspersky and aims to inspire other industry partners to follow the industry best practices.
- providing capacity building efforts to support businesses with knowledge and skills in an ongoing vulnerability treatment process. As mentioned earlier, examples could include Kaspersky's Cyber Capacity Building Program[8] – the dedicated training program that includes modules where we share best practices for vulnerability management and CVD as well as share our experience in handling vulnerability reports from the research community; which many government attendees have found useful.
- encouraging businesses – both manufacturers of software and hardware – to use coordinators (through bug bounty programs) for coordinated vulnerability disclosure (CVD);
- creating financial incentives and benefits, e.g., through ensuring more beneficial terms in cyber insurance programs for businesses with well-established and maintained vulnerability management and disclosure processes.

What other approach could be taken to improve supply chain management for small businesses?

In addition to a cybersecurity health check program to improve Australia's cybersecurity, we would also recommend:

- encouraging both manufacturers and consumers of ICTs to enhance software component transparency by developing/maintaining/providing (for manufacturers) and by requesting (for consumers) Hardware and Software Bills of Materials (H/SBOMs). Currently the US

[7] https://www.oecd-ilibrary.org/science-and-technology/encouraging-vulnerability-treatment_0e2615ba-en
[8] https://www.kaspersky.com/capacity-building

NTIA drives the multistakeholder process on sharing the best practices in H/SBOMs and has recently published the minimum elements guidance[9], which could be used by industry.

- developing and providing guidance on best practices in supply chain risk management (SCRM) and specifically identifying the bare minimum optional security controls that need to be taken by businesses;
- supporting businesses with capacity building efforts and training programs.

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?

Currently Australian consumers remain not sufficiently protected from cybersecurity failings or shortcomings arising while they are using digital products or ICTs (other than what the current Privacy Act requires). As mentioned above in our input to questions earlier, it is necessary to further educate consumers about rights and appropriate channels for reporting their issues with digital products in an easier and less cost-consuming way.

Conclusion

We remain at your disposal for any clarification required in regard to this submission and remain available for discussion on how we could be of service to Australia in ensuring successful implementation of its cybersecurity policies. To that end, please feel free to contact our Head of Public Affairs, APAC, Ms. Genie Gan, at [redacted]. Thank you.

About Kaspersky

Kaspersky is a global cybersecurity company founded in 1997. Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky technologies and we help 270,000 corporate clients protect what matters to them most. Learn more at www.kaspersky.com. To learn more about Kaspersky intelligence reports or request more information on a specific report, please contact [redacted]

[9] https://www.ntia.gov/files/ntia/publications/sbom_minimum_elements_report.pdf