Notitia
Cyber Security Strategy
Discussion Paper

April, 2023

Notitia

Notitia is a national leader in end-to-end data analytics and digital transformation.
Our people solve real world problems, providing analytics, design, development and strategy for more than 60 clients. Notitia provides information and insights based on our expertise and experience in data strategy, data quality, analytics, data governance and cyber security.

This is Notitia's submission in response to the 2023-2030 Australian Cyber Security Discussion Paper, written by Notitia Managing Director & Founder Alex Avery and Notitia Director Lisa Byrne.

Working across a broad range of industries and sectors, Notitia has a unique insight of Australia's cyber security issues from both a business and governance perspective. We see it as our obligation to present our views, on behalf of our clients, and their future success in implementing effective cyber security measures, to protect their business and their customers.

Notitia welcomes this opportunity to comment on this critical and timely strategy.

Alex Avery

Notitia Founder and Managing Director
Alex is passionate about applying analytics for societal benefits, having worked across Australian and global startups, Big 4 consulting and academia. He's an Honorary Research Fellow (University of Melbourne) and is across all things data.

Lisa Byrne

Notitia Director
Lisa has 30 years' industry experience in Finance, Data Governance, CyberSecurity and Master Data together with MBA, CPA and GAICD qualifications with specialist skills in developing Business Intelligence solutions - including data warehouse/data lake project management and business process optimisation.

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?

As outlined by the Minister, the case for change is clear. Australia has a patchwork of policies, laws and frameworks that are not keeping up with the challenges presented by the digital age. Like many other countries, Australian businesses and citizens produce and use a lot of data. This volume of data has significantly increased in recent years, with projected future growth. As well as being cyber secure, this strategy should aim to increase cyber awareness within corporates and individuals. This strategy needs to increase awareness, as well as security, which means both suppliers and consumers all have a role to play and as stated in the discussion paper, "All of us must play a role in keeping our critical data, systems and infrastructure safe".

This strategy's success hinges on the ability for customers to hold businesses accountable which relies on the awareness of cyber security. Notitia Director Lisa Byrne has backed this position in the media, quoted by Startup Daily March 16, 2023 and during an interview on Startup Daily TV and Ausbiz March 20, 2023.

Concept:

- Policy-enforcer-to-business deterrents, will only take us so far, customers also need to be empowered to hold businesses accountable.

- If Australian consumers expect businesses and institutions to prove their security, before data is handed over, the power of consumer spending will dictate the importance that all businesses place on adequate data security.

Tactical actions:

- Investment in a targeted consumer education campaign to make it easy for consumers to know where to spend their money and who to hand over their private data.

- As customers, we all need to be brought into the conversation, educated and informed of what we should expect from any business and institution that we engage with.
- Educating the public on what the business requirements are for their data to be protected and the risks involved in handing their data over to a business that does not have an adequate data security plan.
- Targeted marketing/education campaign which prompts consumers to look for that “tick of approval” in the same way they would only buy a child’s car seat from a manufacturer who meets safety standards.
- A way for businesses to easily market their compliance and for customers (both domestic and international customers) to feel confident in checking. This could be a public data security compliance register, along with certified compliance logos on website footers or forms. This approach has already been used successfully:

WE'RE COVID SAFE
Compliance Australia Certification Services
SAFETY
AS/NZS 4801
AUSTRALIAN MADE AND OWNED

- Each business should have to go through the process of meeting all the cyber safety requirements and proving that they have them in place, like an ISO9000 set of five quality management systems (QMS) standards.

US considerations:

- Consideration should be given to the US approach that includes federal spending towards a mandate to protect medical devices from hacks or ransomware attacks. This legislation explicitly states that companies cannot sell their connected medical devices without first showing the Food and Drug Administration (FDA) a solid cybersecurity plan. This budget also allocates significant funding to the FDA to enable the organisation to keep up with rapidly-evolving security threats.
- Unlike the US, Australia currently doesn’t have clear mandatory minimum cyber security standards for businesses. There are a multitude of frameworks that can be adopted and used by Australian companies.
- US-based federal agency, the National Institute of Standards and Technology (NIST) helps businesses of all sizes to better understand, manage, and reduce their cybersecurity risk and protect their networks and data. NIST frameworks are used to measure an organisation’s current state of cybersecurity and strengthen its security posture. All federal government agencies and any federal contractors (and subcontractors) handling government data in the US must be NIST-compliant. This framework could be considered by Australia.

Australian examples:

- Extend the proof-of-concept Scam Indicator pilot, Telstra and Commonwealth Bank collaboration, that helps to protect joint customers of Telstra and CBA from phone scams. The pilot protects Telstra customers who are on the phone, during a live banking session. It watches for signs that the customer might be the victim of a phone scam, which notifies the CBA to put additional protections in place, before it’s too late.
- Incorporate ideas from the NSW DigitalID, MyGovID solutions. Aim to have one single DigitalID solution for all Australians and organisations which is recognised both within Australia and globally. Streamline compliance within the community, individuals and organisations.

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

C) Should the obligations of company directors specifically address cyber security risks and consequences?

Yes. Notitia believes it is critical that the obligations of company directors specifically address cyber security risks and consequences.

- All company board members should know the role that holds specific accountability for cybersecurity, and is obligated to address cyber security risks with consequences. Meaningful change can only be executed with backing from decision makers, such as a company directors.

- As with all director responsibilities, company board members should also have a solid and current understanding of cyber security, including best practice, as well as those obligations and risks of the company of which they are a board member.

- It should be a mandate for directors to have a current (proactively reviewed and maintained) Cyber Security policy for the organisation. This includes a tested and robust "crisis" response plan.

- The Position Description of the role that holds specific accountability for cyber security explicitly incorporates that accountability and responsibility within that Position Description.

- Directors should view cyber security and corporate governance (the umbrella under which cyber security sits) as a whole-of-business matter. Implementing cyber security is a company-wide approach, not just something that an IT department executes in a silo.

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?

From Notitia's perspective, the burdens on business will be the cost and resources required to implement and then to continually review and improve business processes.

The team at Notitia have observed that there are instances of duplication and/or mixed messages (designed to assist with cyber security confidence) and that places an additional burden on businesses, as well as consumers.

Some issues include:

- Lack of expertise within the business & having to find this experience externally

- Ongoing cost that has not been budgeted.

- Education/awareness gap around what is required/involved in meeting the regulations.

- State Governments executing siloed, state-based cybersecurity solutions, such as NSW's Digital ID.

- Unnecessary data information collection (due to businesses and institutions working in silos and lack of an overarching process) for example businesses that request "proof identification" which has already been provided and validated by a financial institution in order for a customer to open a bank account.

Tactical solutions:

- Appoint a representative advocate, on behalf of Australian businesses, to continually review/monitor and allow for two-way feedback about the regulatory burden.

- Take good/bad learnings from the structure of an international independent body to standardise steps and create a culture shift, to help businesses to meet best practice.

- Make it easy for industry service providers to help businesses to meet the new cyber security obligations. Notitia is well equipped to assist its clients to meet the expectations of the future strategy. How can businesses find service providers who are qualified to implement data strategies (such as Notitia) and feel confident that the service provided will meet their needs? Would there be a "certification" or government register of vetted providers for example?

- Stage the obligations, over a number of financial years, to allow businesses to find the resources they need and pay for the costs.

- The implementation of an overarching "proof of identity" scheme. This would ensure that once "proof of identity" has been verified via an official process (say, to open a bank account) other businesses/ institutions should be able to request a reference from that institution as verification. This would prevent multiple institutions from requesting the same information from a customer and storing it within their IT infrastructure (therefore increasing that individual's cyber security risk). As an example, some individuals were customers of Medibank, Optus and Latitude and their data has been compromised three times with the data breaches of those institutions.

5. How should Australia better contribute to international standards -setting processes in relation to cyber security, and shape laws, norms and standards that uphold responsible state behaviour in cyberspace?

There are 41 international accounting standards laid out by the not-for-profit International Financial Reporting Standards (IFRS). Currently, it does not appear that any of those standards cover accounting's role in managing cyber security.

Notitia has a unique insight into how accounting and cyber security interplay, with our Director Lisa Byrne starting-out as a Certified Practising Accountant. Lisa's background in accounting, finance and business has underpinned her career in data strategy, data quality, data governance and cyber security.
Notitia believes that Australia could lead by example, in incorporating and shaping the role that accounting has in maintaining cyber security.

According to IFRS the "G20 and other major international organisations, as well as very many governments, business associations, investors and members of the worldwide accountancy profession, support the goal of a single set of high-quality global accounting standards."

Input into these global accounting standards is an ideal vehicle to achieve global consistency in understanding and managing cybersecurity.

11. Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?

Not only should Australia look to implement a tailored approach to uplifting cyber skills, beyond the broad umbrella of STEM, but

Notitia strongly supports particular focus on using initiatives to boost female participation in this sector.

Notitia's commitment to gender equality in the workplace, is demonstrated by our 46% female workforce (achieved across both our executive and broader team), our extended parental leave policy, flexible working arrangements and part time workforce (supporting our employees to pursue other interests or work while raising young children).

In 2022 females accounted for 27% of the STEM workforce (according to the Federal Government's STEM Equity Tracker).

According to AustCyber, in the 12 month period up until May 2022, there were 14,925 full time cyber security job openings, with only 891 part time job openings.

Notitia has committed to a number of initiatives to increase the diversity (including gender diversity) within our organisation.
This includes:

1. Visas to employ individuals with the appropriate skills that are not Australian citizens and, in turn, increase the depth of diversity of cultures across the organisation.
2. Maintaining gender diversity. Notitia is close to a 50% female workforce (46% across our team with a 50% split within our executive).
3. Diversity of skills and backgrounds, in our team we also have PHDs in health science, neuroscience, biomedical science, a CPA and degrees in design and communications.
4. Team members at all levels of seniority can work flexibly and part time.
5. Paid roles and opportunities are available within Notitia to those who are changing careers and not following a traditional IT career path, and to support the career advancement for "women in tech".

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?

Based on the assumption that it is highly likely that the number of data breaches will increase, real-time, or near real-time, reporting of this information that can be accessed (e.g. via a portal) will enable the following:

1. Visibility and known reference point for cyber security incidents to stakeholders so they are not reliant on information provided by the organisation which has been the target of that cyber security incident.
2. Ability to incorporate that information into reporting and dashboards, as it is likely to become a key metric reported by organisations to its customers.

15. How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime?

Sharing anonymised information (best practice knowledge, behaviours and support of victims of cybercrime) between government and industry sectors would assist individuals (consumers) to make informed decisions and allow victims of cyber crime to access up-to-date information in one location.

It could be achieved by maintaining a database of cyber security best practice knowledge and behaviours, current situations and actions, which can then be accessed by subscribers (either at a fee or pro bono) to that service.

An example of that concept is Google reviews.

How many times have you referenced and relied on the views of others to select (or not!) a product or service?

a) What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?

- Clear obligations laid out to all businesses.
- Clear criteria to meet the different levels of cyber security safety to then be able to claim levels of compliance (laid out to all businesses). Similar to what is presumably required for a company to be able to use one of the following example logos:

WE'RE COVID SAFE
Compliance Australia Certification Services
AS/NZS 4801
SAFETY
AUSTRALIAN MADE AND OWNED

- Education and training to debunk the myth that small businesses are not the target of cyber crime.
- Free resources and training for small businesses to upskill and train their employees.
- Access to creditable/certified providers that provide cyber security products for free or low cost.
- Staged-implementation to ensure that small businesses are able to implement appropriate actions in specific timeframes.
- Grants for small businesses who have demonstrated the desire to improve their cyber security and need the assistance to put into place.
- Sharing of techniques and approaches used by businesses to incorporate and meet various requirements for implementing appropriate actions.

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?

- Australian cyber security startups receive 300 times less funding than international peer leaders, according to AustCyber's Sector Competitiveness Plan 2022.
- Learning from high cyber safe ranking countries such as Denmark, to create overarching objectives that direct the priorities of the myriad of participants within the cyber ecosystem.
- Ensuring strategy uptake through targeted communication campaigns to cater for the many audiences within the ecosystem including small, medium and large organisations, service providers and consumers.

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

The strategy needs to be regularly reviewed and updated, given the speed at which cyber security incidents and sophistication of those incidents develop, as well as the speed at which technology develops.

Having a well understood and robust framework to guide that review process is akin to the development of an appropriate Data Governance Framework for an organisation. The central theme and purpose will not alter. However, the design, escalation process and approach will vary, based on what is required, and what will resonate with the target audience and stakeholders.

20. How should government measure its impact in uplifting national cyber resilience?

- Create clear quantifiable measures.
- Establish a baseline in the first year.
- Continually re-run the measures every X months to show trends.
- Be consistent in the definition of the metric and how often it is measured.
- Easily accessible, clear, regular and broad communication of performance against the quantifiable measures

Clearly quantifiable measures (such as a % of Net Revenue) are needed to uplift national cyber resilience.

A baseline would be established in year 1, with the same measures repeated and reported every X months to show trends.

Consistency is key, along with a comprehensive definition of the metric and how often this metric is measured and reported.

This metric would also be a key reporting item included in regular internal reporting / management accounting reporting and reflected in regular analytics/reports/dashboards provided internally and externally.

21. What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?

The government needs to consider building a portal to report all cyber incidents.

Real-time or near real-time refreshing of this data and real-time or near real-time reporting of this information that can be accessed by the public.

Given that the size and/or frequency of the cyber security incidents is likely to increase, it is likely to become a key metric and reference point for Australians.

This removes the current reliance of affected and potential affected individuals on information provided by the organisation which has been the target of a cyber security incident.

The ability to incorporate that information into a portal, dashboards and reporting is a service and skillset of Notitia.

Notitia has undertaken similar activities for clients using other publicly available information such as ABS data so that businesses are able to obtain a better understanding of their customers and/or target customers and/or services.