VeroGuard Systems

Ms Kendra Morony
Assistant Secretary
Strategy, Governance & Industry
Cyber Security Policy Division
Department of Home Affairs
4 National Circuit,
Barton ACT 2600

8 November 2019

Australia's 2020 Cyber Security Strategy' – A call for views.

Dear Sir/Madam,

Please find attached our response to 'Australia's 2020 Cyber Security Strategy' – A call for views.

We welcome this initiative and have attempted to be succinct in our response.

We believe that the approach to cyber security - protecting data, digitised assets and privacy, has not only been inadequate to date, but also missing the key ingredients to allow the internet to be a safe and secure environment for business and citizens.

The statistics and forecasts of losses from cybercrime, clearly bear this out and we believe that the government has a real and immediate opportunity to address this by focusing more on the regulatory landscape and underlying infrastructure for the internet.

We are happy and available to discuss further.

Yours Sincerely,

H. Daniel Elbaum
Chairman and Co-CEO
VeroGuard Systems

1. **What is your view of the cyber threat environment? What threats should Government be focusing on?**

VeroGuard believes that the threat from cyber-crime to global economies has the potential to be larger in each year from 2020 than the entire impact of the global financial crisis of 2008/9. The Global Risks Report (2019) of the World **Economic** Forum (WEF) predicted that **cybercrime** will be costing the global economy $**6 trillion** by 2021.

Organisations are being driven to increasingly participate in the digital economy to improve experience and efficiency for employees, customers and suppliers. This shift is exponentially increasing sovereign and whole of economy risks.

What threats should Government be focusing on?

Identity theft and unauthorised data acquisition.

a. **Identity** - No government, business or private citizen is immune from cyber-attacks and the responsibility of data and identity security remains with the technology user and not with third party service providers.
"Our identities and what we have access to are the new keys to the kingdom, which, currently can be here, there and everywhere. With identity set in place as the new gatekeeper, organizations can be vigilant to emerging security threats and ready for the new reality of our digital age" [1]

b. **Data security**
Data breach statistics[2] clearly tell us that the use of cyber-crime detection and response solutions are not providing adequate protection for organisations data that has been exposed to online systems. Further it has become more important than ever for data integrity and management to be at the top of any organisations priorities not just for matters of privacy and risk but also due to the way we are using data as a foundation to making critical decisions driven by modern analytics and intelligence tools. It is critical to note that data and identity are two sides to the same coin (we must trust the provenance and voracity of the data as much as we must prevent the data from being accessed by unauthorised users) Particularly with more organisations including Government, using cloud service providers data storage capacity it is critical that data and user credentials are

[1] - Danny Kibel. Forbes Online. Forbes Technology Council. November 1, 2019

[2] https://www.ibm.com/security/data-breach
https://enterprise.verizon.com/resources/reports/dbir/

managed and secured outside these environments and with the highest possible level of control and security.

2. **Do you agree with our understanding of who is responsible for managing cyber risks in the economy?**

   Yes. Currently there is no evidence that a government, association or organisation is responsible for managing cyber risks in the economy.

3. **Do you think the way these responsibilities are currently allocated is right? What changes should we consider?**

   No. We believe that the Australian Government can (and for the first time has the opportunity) to assert leadership in establishing infrastructure which **prevents** identity theft and data breaches for all Australians. The focus to date has been substantively around **detection and remediation** rather than absolute prevention.

4. **What role should Government play in addressing the most serious threats to institutions and businesses located in Australia?**

   Government must provide absolute protection for identities and sensitive data by establishing secure identity and standards for data at rest that cannot be decrypted by unauthorised users.
   a. The Australian Government can now ensure that cyber policy is regularly updated to reflect the rapidly changing threats of the many levels of cyber risks and crimes.
   b. Develop and implement new protocols for open network security.
   c. Critical Essential Service assets to have immediate upgrades to absolute full cyber threat prevention. (Machine ID, communication and data)

5. **How can Government maintain trust from the Australian community when using its cyber security capabilities?**

   Adopt and distribute a platform that provides non-repudiable digital identity and data security that does not allow decryption by unauthorised users nor compromise the Governments and citizens agreed privacy standards. Provide cyber security upgrades which prevents incursion to critical assets of Australia's Essential Services (including Security Agencies). This platform exists which delivers this security, privacy settings and user controls.

6. **What customer protections should apply to the security of cyber goods and services?**

   At a minimum the Government can establish and publish a new table of cyber security protocols (standards) to provide transparency of the performance and effectiveness of readily available cyber security products to address specific issues of cyber security enabling end

users with the ability to choose their security level. This way government and business can dictate who and interact with it and their minimum platform system requirements.

7. **What role can Government and industry play in supporting the cyber security of consumers?**

   Government must provide absolute protection for identities and sensitive data by establishing secure identity and standards for data at rest that cannot be decrypted by unauthorised users.
   a. The Australian Government needs to ensure that cyber policy is regularly updated to reflect the rapidly changing threats of the many levels of cyber risks and crimes.
   b. Develop and implement new protocols for open network security.
   c. Critical Essential Service assets to have immediate upgrades to absolute full cyber threat prevention. (Machine ID, communication and data)

8. **How can Government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings?**

   Government must provide absolute protection for identities and sensitive data by establishing secure identity and standards for data at rest that cannot be decrypted by unauthorised users.
   a. The Australian Government can ensure that cyber policy is regularly updated to reflect the rapidly changing threats of the many levels of cyber risks and crimes through its agency ACSC.
   b. Test adopt and implement available new protocols for open network security.
   c. Immediately upgrade critical essential service assets to absolute full cyber threat prevention. (Machine ID, communication and data)

9. **Are there functions the Government currently performs that could be safely devolved to the private sector? What would the effect(s) be?**

   Yes. However, the responsibility for accrediting systems, platforms and at what level should remain with a trusted source like government.

   The market and the commercial pool of innovators often works with agents of the government like CSIRO and should be encouraged. Dedicated investment by government on specific technology gaps to encourage focus by Australian tech companies.

10. **Is the regulatory environment for cyber security appropriate? Why or why not?**

    No. Policies and standards used today are outdated. Rapid changes to and in technology obsolete frameworks and protocols in relatively short cycles. Cyber-criminals exploit these gaps because policy focus is on detect and mitigate rather than prevention.

11. What specific market incentives or regulatory changes should Government consider?

Australia has been relatively successful at providing early technology development incentives, but mostly unsuccessful at enabling early technologies to mature through an innovation pipeline. Likely causes are the lack of leadership with a whole of government approach to prevention of cyber incursion. The current federal departmental siloed approach to their own cyber security is counterproductive to a focussed national solution. This must stop.

With this vacuum of national accountability and the fragmented budgets and responsibility that goes with it, many companies and technologies simply wander off to other markets and the intellectual property leaves Australia. Cyber Security is fundamental to the success of the Australian economy. Government should take an important role in assessing and testing emerging cyber security technologies that focus on complete protection rather than post incursion management.

12. What needs to be done so that cyber security is 'built in' to digital goods and services?

It has been widely proven that varying standards of digital security, technology interpretations of security methods, conflicting agendas of digital giants and the general lack of an identity layer for the internet has placed the digital economy at a crisis crossroad. Not limited to but including:

- The largely experimental adoption of biometrics has led to unprecedented and growing identity privacy and security breaches.
- Regular updates and varying standards of smartphone security and user management expose all smartphone connected systems and data to high numbers of breaches.
- Machines that are now connecting to the internet have never been designed with the level of cyber security required to withstand today's cyber criminals.

Government must provide absolute protection for identities and sensitive data by establishing secure identity and standards for data at rest that cannot be decrypted by unauthorised users.

a. The Australian Government needs to ensure that cyber policy is regularly updated to reflect the rapidly changing threats of the many levels of cyber risks and crimes.
b. Develop and implement new protocols for open network security.
c. Critical Essential Service assets to have immediate upgrades to absolute full cyber threat prevention. (Machine ID, communication and data)
d. Digital ID for humans and machines **must be** 'out of band' to avoid access from standard operating environments.

13. How could we approach instilling better trust in ICT supply chains?

Government must provide absolute protection for identities and sensitive data by establishing secure identity and standards for data at rest that cannot be decrypted by unauthorised users. Users across the supply chain must have the same level of confidence in their supply chain as they do in their own systems.

14. How can Australian governments and private entities build a market of high-quality cyber security professionals in Australia?

Decide a protocol, adopt a platform, standardise systems and roll out common criteria to participants in Australia that moves the Country to the next generation of cyber security. Once adopting the leading platform for cyber security worldwide, Australia will become a global exemplar for cyber security that unifies education institutions, policy makers and IT associations.

15. Are there any barriers currently preventing the growth of the cyber insurance market in Australia? If so, how can they be addressed?

Yes. Because of the exponential rise in loss associated with cyber-crimes the insurance market is reeling to understand how to underwrite its risk and has largely become incapable of providing quantifiable premiums or adequate coverage for business. Insurance markets rely on the ability to identify and measure past and potential losses. This existential threat to business needs a way to quantify the threat to change this dynamic.

The adoption of a platform that eliminates compromised credentials and stops unauthorised access to data in the cloud will provide an environment to allow common insurance practices to be adopted.

16. How can high-volume, low-sophistication malicious activity targeting Australia be reduced?

Government must provide absolute protection for identities and sensitive data by establishing secure identity and standards for data at rest that cannot be decrypted by unauthorised users.

a. The Australian Government needs to ensure that cyber policy is regularly updated to reflect the rapidly changing threats of the many levels of cyber risks and crimes.
b. Develop and implement new protocols for open network security.
c. Critical Essential Service assets to have immediate upgrades to absolute full cyber threat prevention. (Machine ID, communication and data)

d. Digital ID for humans and machines **must be** 'out of band' to avoid access from standard operating environments.

17. What changes can Government make to create a hostile environment for malicious cyber actors?

Mandate the use of secure digital ID. Hardware Security Module (HSM) to HSM ID management and communication. Implement data storage that cannot be accessed by unauthorised users (particularly in the cloud).

18. How can governments and private entities better proactively identify and remediate cyber risks on essential private networks?

The Australian Government has available to it a class leading Australian developed in conjunction with the CSIRO Data61 a preventative platform which is now available to all Australian governments, business and the community that delivers a significantly higher efficiency level to monitoring and detection tools than in the global market today.

19. What private networks should be considered critical systems that need stronger cyber defences?

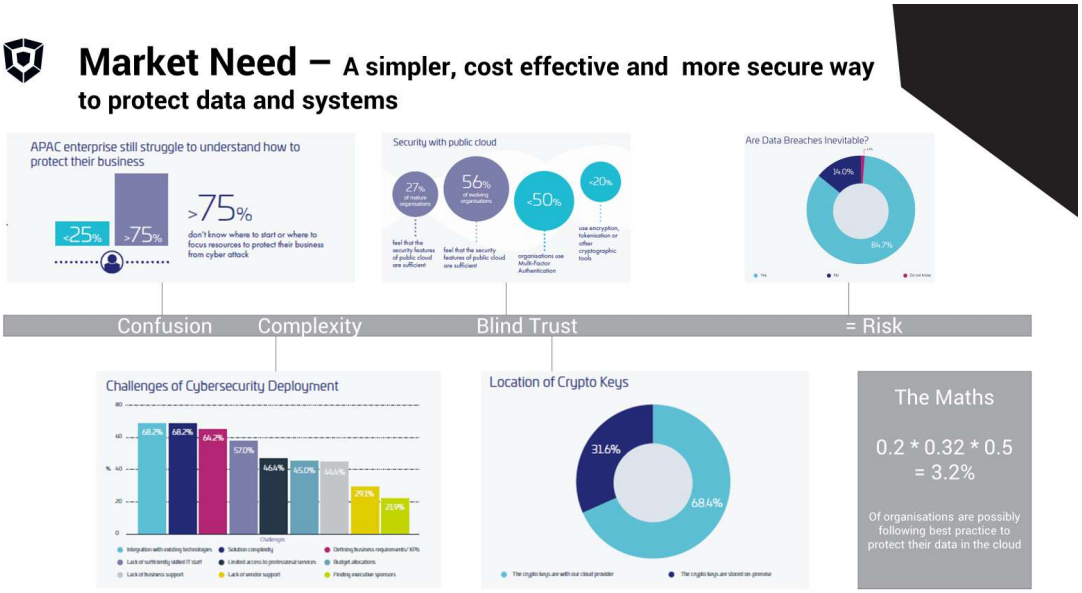
All Essential Services operated by contractors to federal and state governments and private sectors should have the highest priority including (but not limited to) defence, border protection, financial, energy, communications, health, welfare and emergency services.

20. What funding models should Government explore for any additional protections provided to the community?

The Australian Government has an opportunity to coinvest in a Public/Private Partnership to deploy a preventative (infrastructure) platform across Government and the community which is indigenous to Australia but with a global application.

21. What are the constraints to information sharing between Government and industry on cyber threats and vulnerabilities?

Currently constraints are largely self-imposed as government and organisations restrict sharing of sensitive information out of security concerns, an abundance of caution or simply a lack of clarity, knowledge and or skills about the threats and vulnerabilities. Business and Government are also not clear on where to start and what solution to adopt from the problem if they are able to identify the problem. This means that they do not prioritise sharing or participating in the right forums.



22. To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings?

Strongly Agree.

23. How can an increased consumer focus on cyber security benefit Australian businesses who create cyber secure products?

Cyber security protection is a grudge purchase by consumers and the majority have little knowledge of how to extinguish risk. Assertive policy by government is required on how consumers interact online and what they can do to fully protect their ID and data. A heightened consumer focus on cyber security benefits will drive increased investment by organisations to enhance and protect digital interactions. The increased demand by those business for cyber security products **that work** will underpin the continued investment by specialist class leading innovators to stay ahead of future threats with products that in turn protect global economies.

24. What are examples of best practice behaviour change campaigns or measures? How did they achieve scale and how were they evaluated?

Safe and successful adoption of cellular networks are a strong demonstration of how governments successfully deployed, scaled and safely managed a significant behavioural shift in telecommunications. They followed a highly successful model of:

- Setting standards
- Managing identity
- Regulating distribution

- Creating competition
- Creating a trusted environment

In fact history has shown us successful distribution and eventually mass adoption of communication channels including print, postal, radio, telecommunications (fixed and then cellular) and television in controlled ways have had some of the most profound impacts on how our societies safely live and work.

In every case adoption was often predicated on a government assessing the technology, the potential good and bad consequences of the media and how to best apply regulations that protect the interests (including economic, security and welfare) of their country and people. Demand and behavioural changes often followed the successful identification by government and business of the economic and political benefits of adoption and then by citizens who could safely and economically engage with the media.

The internet however came without regulation or a clear understanding by governments around the world about how it would be adopted, the risks it may pose and ultimately how it may evolve. The internet also was famously created without an identity layer, and therefore as the risks became threats and ultimately led to substantial criminal acts, it had become extremely difficult to contain the growing threats and hold perpetrators of those acts to account.

Cyber-security awareness and training remain an important part of an overall strategy to help with cyber-crime, however, it is important to note that security outcomes have not changed even with significantly more money, effort and resources focused on cyber-security education.

It is not too late however to learn from history and establish better frameworks for safe and successful adoption and use of the internet:

- Establishing appropriate regulations to manage identity and communications over the internet.
- Maintain awareness and training but with sufficient controls and ability to identify criminal acts
- Providing business with a secure platform to safely transact and communicate over the internet
- Delivering secure standards for data management that business can easily understand.

25. Would you like to see cyber security features prioritised in products and services?

Yes. All digital interactions development and in market should be assessed and rated on their cyber security class. This means that products need to be classified as either protection, detection or remediation. All these are vastly different in experience of users which need to match their expectation when taking responsibility by purchasing and deploying their security platform.

26. Is there anything else that Government should consider in developing Australia's 2020 Cyber Security Strategy?

Australia can improve its ability to develop and protect its own cyber security capabilities as a priority independent of the rest of the world. This can be done by driving change through federal government leading by example with the adoption of centralised responsibility for the issue and strict protocols of engagement with dealing with it which will drive industry and its citizens to morph to a secure environment. In a very short time Australia can ascend to a global exemplar for national security, surpassing Estonia as a class leading country in cyber security.