Australian Government
Department of Home Affairs

November 1st, 2019

Response to Australia's 2020 Cyber Security Strategy - Call for Views

Introduction and about GROW

GROW is excited about the opportunity to contribute to Australia's 2020 Cyber Security Strategy. We welcome any advances in our country's security strategy to make us more resilient in an ever-changing cyber landscape and are pleased to see the Government taking this important issue seriously.

GROW is a new market entrant in the superannuation services industry. The company has been in operation for three years and provides innovative superannuation product offerings, as well as delivering administration platform capability on distributed ledger technology and holistic administration services to client funds.[1]

As a technology-oriented start-up, GROW has recognised early the critical importance of implementing the correct settings on cyber security. GROW ensures that cyber security considerations drive system design and controls, and cyber security represents a disproportionately high amount of the organisation's investment.

Our observation is that the quality of an organisation's cyber defences is driven by the level of commitment to prioritising information security and the quality of its personnel. The size and history of an organisation are rarely an accurate measure of how secure a company's systems are likely to be. In fact, larger organisations face enormous operational hurdles when trying to respond rapidly to emerging cyber threats.

Accordingly, we believe GROW is uniquely placed to comment on cyber security in the context of the superannuation industry, which is a sector that manages the data of millions of Australians saving for retirement. With that perspective, GROW offers the following comments for the Government's consideration.

Citizens deserve cyber security essentials

In November 2018, French President Emmanuel Macron launched the Paris Call for Trust and Security in Cyberspace, calling for the development of common principles securing cyberspace. The document currently has 564 official supporters, including nation states and private businesses. Support for the initiative has been encouraging, but the document itself lacks specifics and fails to provide truly game-changing actions.

[1] Australian Financial Review "GROW Super to offer hybrid pension product" 30 October 2017 and Australian Financial Review "IOOF takes stake in start-up super fund GROW Super" 12 February 2018

That said, the dynamic of having stakeholders across Government and Industry contributing to a shared standard is very valuable. A similar Call for Security, more tailored to the needs of Australian businesses and borrowing from standards such as CPS234 and even SOC2, could potentially go a long way in establishing a like-minded collective of Australian stakeholders willing to invest in cyber security.

This would offer citizens minimum cyber security expectations when they participate in the digital economy.

In GROW's view, stakeholders should represent Government, regulators, cyber experts, Industry and consumer representatives. GROW is keen to meet with Government to suggest ways to establish and then progress such an initiative.

Specific cyber security considerations

GROW also offers observations on some of the specific questions in the Government's Federal Cyber Strategy consultation.

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

Services are becoming increasingly digitised. This is particularly true of the superannuation sector with many funds entrusting data to service providers, such as GROW. The risks of unauthorised access to these data stores are increasing with malicious actors advancing new threats constantly.

The Government is right to be focussing on the cyber threats faced by holders of large amounts of PII, which might be companies with thousands of employees or organisations holding data of millions of members or customers. However, clear guidelines are needed to help educate as well as support these organisations to protect their data holdings.

As a service provider in the superannuation market, GROW often plays the role of assisting its clients in better facing today's cyber security threats. Some clarity regarding Government's expectations for 'data-heavy' sectors like financial services or superannuation would be welcome.

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

The concept of "technical debt" has long been applied to software development, to refer to the additional work that is created further down the line when teams take an easy solution instead of developing a more difficult, but more scalable solution. A similar concept applies to cyber security, wherein companies that neglect to implement security into their product or service now find it much more difficult to secure their product later. "Security debt" is rife among many large companies.

Due to its nature, security debt is much simpler to prevent than to remediate. While much of the responsibility for security within companies lies with the managers, it starts with the developers - and the unfortunate reality is that many software developers are not educated on security. Cyber security courses aren't a requirement in many Australian universities, meaning that many software graduates are not sufficiently educated in relation to how to build a secure product.

While the Government already has outreach programs aimed at encouraging more students to study cyber security, there is no initiative on educating those who have already decided to study software development. Creating initiatives that enable computer science students to be more involved in security and encouraging universities to do more could potentially prevent more security debt being accumulated in the future.

The Government could also encourage "secure by design" approaches by offering recognition to companies that invest in design choices that prioritise security considerations. GROW's offerings are based on inherently secure distributed ledger technology, which offers a combination of security and scalability.

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

There has been significant discussion regarding what appropriate cyber security standards for the superannuation industry could entail. Superannuation accounts contain material volumes of PII, and until now, there have been few publicly announced cyber security breaches in the industry. However, this is in part due to the non-connected nature of the legacy technologies the majority of the industry continues to utilise. There remains material risk that, as the industry transitions to the digital economy, these data holdings become exposed.

GROW recommends that Government resist any calls to treat the superannuation industry separately. To ensure an aligned approach across financial services and the economy more broadly, Government should set high standards but those standards should apply equally across sectors. If Government considers that the networks and data systems that underlie superannuation should be critical systems, GROW recommends that the assessment be conducted on the same basis as a critical system in logistics or communications.

Next steps – discussion and consultation

Security is fundamental to a vibrant digital economy and GROW is delighted that Government is bringing focus to this important issue.

As a proposed next step, GROW would be keen to participate in any consultations that Government decides to run on this area of policy. If any of the positions proposed in this paper are of interest to Government, GROW would be pleased to provide further context and analysis.

Regards,

David Baxter
Chief Technology Officer

Katerina Borodina
Cyber Security Lead