FS-ISAC

TLP WHITE *

FS-ISAC Response – Australia’s 2020 Cyber Security Strategy

A call for views – An FS-ISAC Perspective

|* A description of the Traffic Light Protocol is at Appendix 1 to this document

Intentionally Blank

FS-ISAC
12020 Sunrise Valley Drive, Suite 230
Reston VA 20191 USA

1st November 2019

Cyber Security Policy Division
Department of Home Affairs
4 National Circuit Barton ACT 2600

To Whom It May Concern.

The Financial Services Information Sharing and Analysis Centre (FS-ISAC) represents an organisation that was established twenty years ago to facilitate the sharing and collaboration of active, timely, relevant and actionable intelligence.

At a time when trust has become a vital asset for business, trade and commerce, the Financial Services Information Sharing and Analysis Centre (FS-ISAC) is dedicated to reducing cyber-risk in the global financial system. Serving financial institutions around the globe and in turn their customers, the organisation leverages its intelligence platform, resiliency resources, and a trusted peer-to-peer network of experts to anticipate, mitigate and respond to cyberthreats.

Established as a construct to support critical national infrastructure in the United States, the ISAC model was designed to empower industry verticals to operate and grow in a secure environment underpinned through collective defence against local and foreign based entities. Accordingly, whilst the views expressed in this response reflect a financial industry perspective, they do in large represent a much broader view of the cybersecurity landscape.

This document forms one of two submissions in response to the call by the Department of Home Affairs and the Australian Government for all 'interested parties' to 'participate and contribute in the development of the new strategy'. This TLP WHITE response is categorised under the Traffic Light Protocol used by FS-ISAC and its definition is detailed at Appendix 1 to the submission document.

The views expressed in this response reflect solely those of FS-ISAC and should not be viewed as a commentary or opinion of the United States Government or any other body with which FS-ISAC is affiliated. However, it should be clear that our global membership places FS-ISAC in a unique position to offer a global perspective on the nature of cybersecurity and the threat posed by a nation-state, other actors, and criminals alike against the global financial community.

Should you require further discussion with FS-ISAC please contact Scott Ainslie, the FS-ISAC Regional Director - Australia and New Zealand ([redacted]) should you have any questions or require additional information on this submission.

Narrative

Positioning ourselves for the future

Where are we now?

Questions

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

Response

The cyber threat environment has grown significantly in the past decade as a direct consequence of ubiquitous technology and the growth of the Internet. The ability for criminals to access personal and private data has grown proportionately with technology development, empowering and assisting them in their activity through the concurrent development of the 'deep' and 'dark' web.

FS-ISAC actively monitors cyber threats towards the financial services sector from a global perspective. Over the years, we have observed diminishing distinctions between threat actor types. A foreign government or government-sponsored groups are engaging in criminal activities for financial gain, and organised cybercriminals are conducting espionage-type operations. The Australian Cyber Security Centre (ACSC) 2017 Threat Report describes two distinct trends reflecting 'sophisticated exploits against well-protected networks' where alternately 'many adversaries, particularly criminals, are targeting networks through known vulnerabilities.[1] Furthermore, the criminal marketplace is continuing to flourish and move towards a more modular economy where customers (even with immature technical ability) can now easily shop the Internet for the tools required to engage in different types of criminal activity. What has not changed is that financial gain is still the most common motive behind data breaches where a motive is known[2], and the finance industry remains a primary target for financially motivated crimes and cyber espionage, threatening individual customers and the economic health of the country.

For the bulk of the threats in the wild, the initial infection vector is currently phishing, email authentication technologies, like DMARC (Domain-based Message Authentication, Reporting & Conformance), providing a level of assurance for companies and individuals that the sender of the email is who they appear to be. Financial institutions report malicious phishing campaigns daily and rely on layered defences to detect them. Phishing without malware can be just as dangerous though. In 2019, insurance giant AIG reported that the number one cyber insurance claim received was for Business Email Compromise (BEC). The term BEC often acts as an umbrella term beyond actual email account compromise and may also include the creation of imitation domains to mimic the real email domain and invoice redirection scams. While there is no malware or exploit kit involved, BEC fraud is often cited as the primary threat to financial institutions and small businesses around the world and can be mitigated through cybersecurity measures and awareness campaigns. The Verizon 2019 Data Breach Report describes this aspect by creating a Financially-Motivated Social Engineering (FMSE) subset that Includes incidents and breaches that featured a Social action but did not involve malware installation or employee misuse[3].

While the finance sector invests heavily in becoming more resilient to cyber threats, not everyone can afford such measures; however, many risks can be mitigated with the extension of best practices. Guides for businesses and individuals to secure themselves can make a significant difference towards achieving a positive outcome. Ransomware attacks have cost municipalities and small businesses billions when taking into account the monetary impact and the aspects of loss of

[1] 2017 ACSC Threat Report (ACSC, 2017, p. 4)
[2] Verizon 2019 Data Breach Investigations Report, date May 2019 (Verizon, 2019, p. 7)
[3] Verizon 2019 Data Breach Investigations Report, date May 2019 (Verizon, 2019, p. 26)

trust and reputational damage. FS-ISAC is a supporting partner of NoMoreRansom, uniting security companies together to develop and make decryption tools freely available to the public. Data breaches from unsecured cloud servers are a near-constant in the media but can be prevented with security best practices, such as self-auditing. Government guidance to enterprises and individuals should be aimed to help the country raise its level of resilience to commonly observed threats.

New technologies are embraced by the cybercriminals as well, but the security response to these new methods can be slow. For example, the adoption of TLS 1.3 can possibly inhibit a security team's abilities to monitor for malicious traffic and many businesses are not prepared for the new environment. When devices in the Internet of Things (IoT) started committing Distributed Denial of Service (DDOS) attacks, the volume of the attacks was considered brand new and DDOS mitigation providers had to adjust for this type of 'new normal'. The advent of 5G will likely enable many more IoT devices to connect to the internet with much faster connectivity, potentially arming DDOS attackers with more potent botnets. Gartner predicts there will be 20.4 billion connected IoT devices by 2020.[4] While regulation over IoT has begun, a significant volume of work remains to be undertaken. Additionally, the government can help predict potential malicious use for these emerging technologies, and to help build mitigation strategies sooner rather than later. 'Organisations with a holistic approach to security will be in a better position to strengthen security defences[5]' and the integration of the Australian government's cyber assets under a single unifying structure, including policy elements, will invariably assist this approach.

Positioning ourselves for the future.

Questions

2. Do you agree with our understanding of who 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?

Response

At present, in an Australian context, there appears to be an element of confusion regarding the roles played by cybersecurity elements within the Australian government, principally regarding the division of responsibility between CERT Australia, ASD, ACSC and the JCSC organisations.[6] The creation of the Department of Home Affairs provided the ability to harness the machinery of several Departments under a single Ministerial Portfolio, however ASD remains under the umbrella of the Department of Defence, and whilst ASD has become a statutory authority it nonetheless remains within the Defence portfolio and reports to that Minister. As all ACSC elements, now including the Digital Transformation Agency, focus on the 'cyber resilience of the Australian community and support the economic and social prosperity of Australia in the digital age[7]' it remains unclear which Minister has prime carriage of cybersecurity as that portfolio has been subsumed by the Minister for Home Affairs. Recognising that it will take some time to coordinate all cyber elements, the need to better inform the business community remains critical and has been lacking.

Government and law enforcement strategies to battle cyber risks are an important part of a country's ability to become more resilient; however, it cannot be allowed to occur in a one-sided approach. The businesses on the frontline experience a regular stream of malicious activity where the majority is not reported externally. FS-ISAC knowledge-sharing is built upon the premise of

[4] Otarris – Article 'Are you prepared to manage all that?' (Otarris, 2019)
[5] Telstra Security Report 2019 - (Telstra, 2019, p. 15)
[6] Which-50 Waves Of Regulation Are Complicating Cybersecurity Strategy (Mallis, 2019)
[7] ASD website – Cyber security - (ASD, 2019)

closed peer-to-peer sharing of events and incidents in a recognition of the need for mutual defence. Often the same actor groups, tools and techniques are observed by the finance sector, albeit usually at different times and from different global regions. Our members learned long ago that they can actually increase the industry's resilience – and therefore their own – when sharing information on various types of threats. We learned to put aside competitiveness for the sake of security. Insight from the private sector is invaluable to understanding the systemic and operational risks facing a country. FS-ISAC engages in public-private partnerships (PPPs) to share trends and understanding of the threat landscape. In our multi-decade experience, the bulk of what happens to the sector on a daily basis does not get shared externally, so FS-ISAC acts as a consolidated point of collaboration for the national cyber security centres and national police agencies.

To understand the risks facing the sector, the government must collaborate with the sector. The application of legislation and regulatory practice may only serve to confuse an industry already burdened with regulation[8]. We understand our own risks and observe on a daily basis how this impacts the industry. In the Australian finance sector, the largest banks are dependent on overseas wholesale funding, making them vulnerable to cross-border transnational shocks. The four major banks hold around 80% of the banking system assets, so the large-scale impact on one or more of them would present a systemic risk to the country. Testing wholesale payments risks show the interdependency not only between banks but between countries. Nearly two-thirds of wholesale funding is from international sources, meaning that payment issues from those sources will present liquidity risks. Risks to New Zealand, the United Kingdom and the United States will likely impact Australia due to cross-border exposure. Approaching the sector with these interconnected risks in mind is necessary to become more resilient.

The creation of the Joint Cyber Security Centres (JCSCs) in the capital cities was an important step towards building public-private partnerships with the various sectors; however, they still lack the rigour for collaborative advances that we have observed elsewhere. Providing for a physical area that private sector can sit and talk to the public sector can extend a PPP relationship greatly, but a formal body of work and information sharing processes are needed to optimise this type of centre. FS-ISAC operates several PPP relationships globally, some of which we place representatives physically into the centre specifically to manage the information sharing flows between the finance sector and government. Joint work needs to be structured at both an operational and strategic level to ensure a common understanding of the threats observed by the critical sectors. Through voluntary sharing of threat trends, the country can start building an accurate picture of the priority threats and those that can present systemic risks to the country.

Governments role in a changing world

Questions

4. What role should Government play in addressing the most serious threats to institutions and businesses located in Australia?
5. How can Government maintain trust from the Australian community when using its cyber security capabilities?

Response

It is generally accepted that the business community does not have the requisite skills to deal with an advanced nation-state attack, and regrettably, statistics reflect a growing trend for nation-state

[8] Computerworld - A trusted marketplace with skilled professionals (Pearce, Cyber security: Sorting through Australia's 'train smash of a legislative landscape', 2019)

attacks to emanate from or under the guise of criminal groups.[9] In this environment support from government is critical to identifying those threats and providing warning or mitigation measures to assist in their detection and mitigation. Earlier this year the Australian Prime Minister announced that 'a sophisticated state-actor had hacked the computer networks of the country's major political parties', and this event was preceded by an attack detected against the Parliament of Australia.[10] These attacks represented a further alarm to the Australian public and business community that Australia was not alone in confronting this threat as even government infrastructure was a target.

In terms of National Critical Infrastructure the Australian Government introduced ground-breaking legislation last year that provided for a mandated national asset register and empowered the Minister to directly intervene where there is an identified risk that is 'prejudicial to security that cannot otherwise be mitigated'. Whilst this particular legislation is focused at protecting critical sectors such as electricity, gas, ports, and water sectors from 'foreign involvement' that could lead to espionage, sabotage, and coercion'[11], the nature of the legislation is such that any critical infrastructure may fall under this approach. Concerns expressed by industry at the time reflected the lack of engagement between the Government and business that would likely impact the ability for the proposed legislation to 'work in reality'.

Beyond the basic cyber education and encouragement to adopt best practices, the government needs to understand how to work with Australian businesses and foreign businesses operating in Australia. Through public-private partnerships and collaboration, government and industry can work together to identify the most significant threats. The government must learn how to work with the private sector effectively; though, this cannot be a one-way relationship. To provide a conducive environment, all parties must build two-way information sharing protocols. The most important role government can play is as a willing partner with private sector, academia and others to battle these threats.

The past year has witnessed the introduction of legislative approaches to the management of cybersecurity that has brought both improved and detrimental impact on the industry. The highest-profile legislative measure was the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act* (*TOLA Act*), which was broadly condemned by industry bodies and despite a broad rejection from all interested parties which was pushed into legislation on the last sitting day of the Australian parliament in December 2018. Commentary at the time from the Department of Home Affairs indicated that 'it did not believe, for example, that the creation of a custom firmware for the iPhone to facilitate access to information on a device would constitute a systemic weakness, that the legislation would not harm the Australian industry'.[12] Recently the Department acknowledged 'that, according to advice it has received from industry, the way the so-called 'encryption' legislation is perceived has had a material impact on the Australian market and the ability for Australian companies to compete globally'.[13.] This statement and the consequent result reflects the difficulties associated when there is a lack of industry experience, respect and knowledge within the policy-making body of government. This parochial approach does little to build a relationship on which trust can be achieved.

The question of trust between public and private sectors evokes a wide range of interpretative response. Its worthwhile to understand just what the term trust represents. 'Trust is closely connected to having positive expectations about the actions of others. When we trust someone, we

[9] Cybercrime Groups and Nation-State Attackers Blur Together (Schwartz, 2018)

[10] International law cannot keep up with cyber-criminals (WEF, 2019)

[11] ZDNet Government passes critical infrastructure national security Bill (Reichert, 2018)

[12] Computerworld 'Australia's 'encryption' law could erode consumer trust in tech: Amazon' (Pearce, 2019)

[13] Computerworld - Government acknowledges Aussie businesses have taken hit from 'encryption' law (Pearce, 2019)

assume that the other will not act opportunistically but take into account our interests'[14]. This interpretation is important as it belies the importance that a human will place in the nature of the relationship and equally defines the level of emotion associated with an action that breaks that trust. An old adage that trust is hard to gain and easily lost is not without truth. To make an assumption that the Government has 'an established trust' with the Australian community is in itself perhaps an optimistic view. The key message from a 2019 PWC report on the 'digital pulse' of the nation revealed that 'Australians are generally neutral in their feelings of trust towards government'.[15] Establishing, maintaining, or restoring trust is a difficult ask, especially where the 'fear of the unknown' impacts a significant proportion of the community. Berg and Keymolen reiterate that 'Trust is inextricably connected to vulnerability' and in a modern world trust may also be placed in systems or technology'.[16]

Over ten years ago FS-ISAC developed what is now known as 'circles of trust', an approach where a far greater number of smaller communities could look to FS-ISAC for information and support. This collateral strength was reinforced when a series of significant cyberattacks targeting US financial institutions originated from Iran. Known as 'Operation Ababil', the attack was conducted in phases over 2012-2013 and reflected DDoS as the attack vector. FS-ISAC provided the support lead in a similar approach to the method used with an earlier Account Takeover Task Force, which proved highly successful as members shared the information necessary to deflect the attacks. Today, the FS-ISAC model reflects three pillars of Intelligence, Resiliency and Trust. This latter element is critical to the successful nature of our sharing and collaboration model. FS-ISAC has been particularly focused on the engagement model with its membership, ensuring transparency and engagement is maintained through an established and ongoing relationship. The 'circles of trust' are also replicated in our 'Communities of Interest' where business groups are formed to assist each other with FS-ISAC facilitation. FS-ISAC has established forums comprising members who drive the agenda and enjoy the rewards collectively through face-to-face meetings and events. The same level of engagement cannot be achieved through webinars or conference calls. The Australian Government's approach to the renewal of the national cyber strategy has sought input from the broader community, this is a good start. However, if a trust is to be reciprocated then the Government must demonstrate that it has listened to industry and community feedback and can demonstrate where its policy and legislation reflects that input.

Enterprise, innovation and cyber security

Questions

6. What customer protections should apply to the security of cyber goods and services?
7. What role can Government and industry play in supporting the cyber security of consumers?
8. How can Government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings?
9. Are there functions the Government currently performs that could be safely devolved to the private sector? What would the effect(s) be?
10. Is the regulatory environment for cyber security appropriate? Why or why not?
11. What specific market incentives or regulatory changes should Government consider?

Response

The previous responses contain much of the information necessary to demonstrate those areas where the Australian Government needs to review its current posture and approach. The impact of

[14] Regulating security on the Internet: control versus trust (van den Berg & Keymolen, 2017)
[15] PWC Digital Pulse – How to fix the government trust issue (Rutter & Khan, 2019)
[16] Regulating security on the Internet: control versus trust (van den Berg & Keymolen, 2017)

globalisation cannot be discounted or ignored when examining the impact that technology has brought to the consumer and business landscape alike. This is a difficult path to follow as technology is invariably complex and crafting legislation to address the concerns will invariably miss the mark as legislation, unlike technology, is anything but agile. In 2017 the Australian Government introduced data retention ('meta-data') laws and reassured the community that access to the data would be restricted to agencies that were hunting for terrorists'[17], only to discover at Parliamentary hearings in the following year that many more agencies were accessing the data than previously stated.[18] This 'leakage' was described as 'authority creep' but the effect was to reinforce a negative connotation in the Australian community that the Government was 'not in control of data security'.[19] Shortly thereafter the TOLA legislation was introduced and passed reflecting a lack of consultation with the community under the banner of national security and the war on terror. FOI documents reveal that the Government disregarded input from tech giants such as Apple, Microsoft, Facebook and Amazon who argued that the legislation was inappropriate, misguided, and would have a detrimental effect on Australian business and the competitiveness of Australian industry in the software market.[20] Digital Rights Watch also argued that many civil groups had been excluded from the process of consultation.[21] John Stanton, Chief Executive of the Communications Alliance stated "Industries are not opposed to national security objectives, only to the mechanisms by which they seek to achieve them if those are damaging to the industry or the public.[22]" Government approaches to dealing with the prickly issue of cybersecurity and its accompanying panniers such as privacy must reflect a much higher degree of consultation and transparency with industry and the Australian community. The Australian government has made important steps with the JCSC program and its engagement with the business community. This is a small step on a long journey that must engage with the business community if it is to be successful. Damien Manuel, Director of the Centre for Cyber Security Research and Innovation suggests seven steps that address strategy, education, small business, industry certification, and that the government must pursue alignment with the ASD 'Essential Eight'[23] in those departments and agencies that have reported breaches or reflect a low-level of cyber maturity.[24] Michelle Price, CEO AustCyber, remarked that the the 'federal government sees cybersecurity as a national security issue, and from that we've got a whole series of legislation that has emerged over the past two years, and there will be more to come. Providing it is adding and compounding that confusion for organisations who are really at the beginning of their cybersecurity journey in Australia'[25]. In essence, Price reinforces industry assertion that the complex relationship between security, privacy, regulations and legislation is creating an environment that is contributing to confusion and 'unintended consequences'. This latter element is reflected in the recent acknowledgement by the Department of Home Affairs that the 'encryption legislation' [December 2018] has adversely impacted on the Australian market'.[26]

Questions

12. What needs to be done so that cyber security is 'built in' to digital goods and services?
13. How could we approach instilling better trust in ICT supply chains?

[17] The Conversation – A steady erosion of privacy (Manuel, 2019)
[18] Parliamentary Joint Committee on Intelligence and Security (PJCIS)
[19] ABC – Metadata laws under fire (Clarke, 2018)
[20] (Pearce, Australia's 'encryption' law could erode consumer trust in tech: Amazon, 2019)
[21] ABC –Encryption laws developed after little consultation (Bogle, 2019)
[22] ABC – Encryption laws developed after little consultation (Bogle, 2019)
[23] ASD – The 'Essential Eight' explained (https:/ / www.cyber.gov.au/ publications/ essential-eight-explained)
[24] Seven ways the government can make Australians safer – without compromising online privacy (Manuel, 2019)
[25] Which-50 Waves Of Regulation Are Complicating Cybersecurity Strategy (Mallis, 2019)
[26] Computerworld - Government acknowledges Aussie businesses have taken hit from 'encryption' law (Pearce, 2019)

14. How can Australian governments and private entities build a market of high quality cyber security professionals in Australia?
15. Are there any barriers currently preventing the growth of the cyber insurance market in Australia? If so, how can they be addressed?

Response

The requirement of 'built-in' rather than 'bolt-on' security in the world of cybersecurity drives a contention that it is much easier to design a product with security from the outset as opposed to adding changes at a later date after the product has reached the market. This concept is not new and is reflected in the frameworks and standards of almost all cybersecurity associated organisations including ISO/IEC standards, IASME, OWASP, ISACA, ETSI, and NIST [27] to name just a few. The approach is also endorsed by industry and engineering bodies such as CMMI, IEEE and the Carnegie Mellon SEI.[28] The emergence of a software development lifecycle originated in the 1960s [29] and was modified by adding security-related inputs to the development phase of the cycle. Regulating that a product must comply with security standards is difficult as addressed previously in this response, 'legislation, unlike technology, is anything but agile'. Market forces in a free Western-style marketplace determine if a product or service is viable and profitable through competitive practice. This aspect remains true for digital products and offerings regardless of the environment in which they are exchanged. If a product goes to market and consumer response reflects a dissatisfaction with the product then they will invariably seek an alternate option or the manufacturer/reseller will make a change to meet the consumer demand. What has changed is the speed of technology development and an expectation from consumers that product improvement through aspects such as software upgrade matches the consumer's appetite for change and improvement. Digital technologies can also influence regulatory approaches. A 2019 joint research report commissioned by the Australian and New Zealand governments examined the opportunities for SME in a digital economy. The report found similarity between NZ and Australian SME in that new start-ups are 'typically small and failure rates for new firms are high'.[30]

Instilling trust in supply chains is a growing problem that reflects multiple levels of complexity. The nature of trust has been described earlier in this response and the aspects reflect a human component and a technology element. In April 2017 PWC and BAE released a report reflecting a global campaign by the APT-10 group targeting Managed Security (Service) Providers (MSP or MSSP). This report revealed the extent to which business and government alike are exposed though the interconnectivity of supply. The attack approach or methodology was not new, although the expressive labelling of the approach as a 'supply-chain' vulnerability took root in public vernacular. In 2013 the Target breach was created through an HVAC supplier to the retailer whose access was manipulated to allow access to the retailers internal POS network. The sheer scale of the breach forced the resignation of the CEO in May 2014, an action that reflected the severity of the loss. The resignation of a high-profile and successful executive galvanized the sector, and for the first time executive boards became 'cyber aware' as this was the first occasion where a data breach had resulted in the resignation of a Fortune 500 CEO[31]. The industry concern generated by the breach, its cost, and the resignation gave rise to the creation of the Retail ISAC. From a functional perspective the Australian government has regulatory powers associated with supply chain management, however, the cyber perspective remains with the provision of education and awareness campaigns to all levels of business and their consumers.

[27] ISO/ IEC, IASME, OWASP, ISACA, ETSI, NIST
[28] CMMI, IEEE, SEI
[29] Elliott & Strachan & Radford (2004) – Introduction to Software Engineering/ Process/ Life Cycle
[30] Joint Research Report – Growing the Digital Economy in Australia and New Zealand – Maximising Opportunities for SMEs (2019)
[31] Washington Post – Target CEO resigns after massive data breach (Douglas, 2014)

Questions

16. How can high-volume, low-sophistication malicious activity targeting Australia be reduced?
17. What changes can Government make to create a hostile environment for malicious cyber actors?
18. How can governments and private entities better proactively identify and remediate cyber risks on essential private networks? *
19. What private networks should be considered critical systems that need stronger cyber defences?
20. What funding models should Government explore for any additional protections provided to the community? *
21. What are the constraints to information sharing between Government and industry on cyber threats and vulnerabilities? *

Response

Basic cyber hygiene continues to be the main approach to reduce malicious activity to individual and corporate resilience. Education must start early and must be continuous. The younger generation is born into a high technology world; however, they still must learn the concepts of individual security, social acceptance of cyber standards and recognition of threats. Phishing remains the most common vector for the delivery of a malicious attack and can be addressed through technology and education. This may not be enough, though, which is why government should develop strong relations with the telecommunications industry, specifically the Internet Service Providers who can action against malicious activity. Large corporations, such as banks and insurance companies, observe this type of low-level activity on a daily basis and can provide massive amounts of data that can be consolidated and analysed to find common patterns and infrastructure.

Enabling ISPs to detect and remediate malicious infrastructure in Australia can help make the system more resilient to hosting malicious servers. Cybercriminals operate across borders and will establish infrastructure for their malicious operations in various countries considered safe from scrutiny. When malicious servers are discovered in Australia, there must be avenues beyond the ISP's abuse box to report and act on these. Repercussions for bulletproof hosters who allow this type of malicious activity should be established as well. Allowing peer-to-peer sharing is another essential feature to build the capability level in the private sector. In areas such as fraud, sharing sometimes clashes with data privacy concerns where the fraudster ends up with greater legal protection than the Australian consumer. Reporting a crime or an attempted crime is part of enterprise's due diligence. Preventing a future crime from occurring can happen through peer-to-peer sharing to share the trends of fraudsters to establish bad accounts and to launder funds.

Critical sectors are usually known and named by the government; however, there must be an assessment of interdependencies. The finance sector, for example, recognises the dependency it has on the energy and telecommunications sector. If a company does not have power or access to the Internet, it cannot operate anymore in today's world. This is especially true for banks. ATM and payments networks form the backbone for day-to-day financial operations for the greater public. If this fails, it leads to unrest and even panic. So, while we understand which companies have the greatest share of the market, we must also consider critical the systems that enables these businesses.

As mentioned earlier, the government cannot engage in one-way sharing and expect it to work. The private sector will not look favourably on what is considered a black hole where there is no apparent return on investment for the effort. This requires a cultural change – a mindset change – for both sides. FS-ISAC has twenty years of exposure learning that collaboration works best when both sides understand what comes from the relationship. This is where structured information sharing comes into value. Whilst the JCSC initiative is a great start, it will not be as successful as they could be without the structure to enable a more collaborative culture. This is not just between government and private companies but also cross-sector and within the sector. Silos exist in many sectors where competition is allowed to usurp collaboration. A culture of collaboration must be fostered to make this work for the nation. This takes years and must be independent of politics. It is essential to build a system that can withstand political change in the government or else this experiment will not last.

There are generally two constraints against information sharing between government and private, namely those that are legally imposed, and those that are perceived or emotive based. The legal imposition generally occurs through an Act that governs the release or control of information such as a national security classification system, whereas the perception or emotive based control is essentially more human and may reflect control, authority, competitiveness or a range of external factors beyond an individual's control. FS-ISAC identified the need for a classification or categorisation system and in 2008 FS-ISAC adopted the 'Traffic Light Protocol'[32] as means to facilitate greater sharing whilst enabling controls on the distribution and management of shared information. This approach allowed member sharing without encountering the controls associated with national security classifications and has facilitated the declassification process for information passed to FS-ISAC through the Department of Homeland Security, the FBI and US Secret Service. It is critical that policy provides the conduit for trusted information sharing, and as previously stated, the sharing must be bi-directional.

Questions

22. To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings?
23. How can an increased consumer focus on cyber security benefit Australian businesses who create cyber secure products?
24. What are examples of best practice behaviour change campaigns or measures? How did they achieve scale and how were they evaluated? *
25. Would you like to see cyber security features prioritised in products and services?

Response

The question of cyber awareness and consumer choice is not naturally connected as decision points on purchasing is influenced by demography and other factors. A survey in the UK revealed that almost half of consumers (46 percent) had done nothing to change their privacy settings on social media despite major breaches on platforms such as Facebook and that less than half had checked to see if their data had been compromised'.[33] A 'Consumer Loss Barometer report from KPMG examined the 'cybersecurity gap between consumers and organisations revealing that over half of the Australian respondents indicated that their personal financial records had been compromised while recognising that device security was a personal responsibility.[34] The report identifies that whilst awareness is growing organisations are not doing enough to advertise the security of their digital products or services.

In the financial services sector, the integration of digital products and services has witnessed explosive growth. As a direct consequence of ubiquitous technology and access to the Internet, a much greater percentage of consumers are shopping online or using digital platforms to transact,

[32] The Information Sharing Traffic Light Protocol (TLP) was created by the UK Government's National Infrastructure Security Coordination Centre to provide a uniform way of handling sensitive material. The FS-ISAC list was adopted by the US-CERT, although they have recently changed to a version adopted by FIRST (Forum of Incident Response and Security).
[33] ZDNet Most consumers have cyber security concerns, but a fraction take action (Brown, 2018)
[34] KPMG Report – Consumer Loss Barometer – The economics of trust (KPMG, 2019)

creating an enormous opportunity for cybercrime to take advantage of the massive data now resident on potentially insecure devices and platforms. The KPMG report identified 'a clear correlation between the relative maturity of the digital transformation agenda and the percentage of consumers who have had their financial information compromised within a region'.[35] Of all the areas in the KPMG report the greatest opportunity for 'securing consumer engagement was the way in which cybersecurity could support organisational growth'.[36]

Marketing a product as 'secure' is difficult at best given its point of origin from manufacturing and its software from a technology perspective, as what is secure today could be compromised tomorrow if a flaw is found or coupled into the device with inherent design vulnerability. High-end software and technology is available through assurance frameworks such as the Common Criteria evaluation, AISEF (ASD), and FIPS (NIST) approaches. However, the additional cost of 'assurance' and the time required for assessment is presently such that it would prohibit general consumer appetite for cost-effective and cost-competitive goods in the marketplace.[37]

Other issues

Questions

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

Response

The nature of how an ISAC operates is relevant to the broader cybersecurity community where public-private partnerships exist. The TISN represents a model architecture that whilst now somewhat aged, continues to reflect a design that is practical and functional. The key element in how to achieve the best from a PPP relationship remains with the need for each party to remain objective and yet engaged, providing a degree of separation that permits each party to engage without the fear of compromise whilst providing a joint outcome that builds into a trusted relationship. This model is discussed further in our AMBER response.

[35] KPMG Report – Consumer Loss Barometer – The economics of trust (KPMG, 2019)

[36] KPMG Report – Consumer Loss Barometer – The economics of trust (KPMG, 2019)

[37] Common Criteria portal, AISEF, FIPS

References

ACSC. (2017). *2017 ACSC Threat Report.* Canberra, ACT: Australian Government Publisher.

ASD. (2019, October 1). *Cyber security*. Retrieved from ASD: https://www.asd.gov.au/cyber

Australian Productivity Commission and New Zealand Productivity Commission. (2019). *Growing the Digitl Economy in Australia and New Zealand - Maximising Opportunities for SMEs.* Canberra/Wellington: Commonwealt of Australia nd New Zealand Crown.

Bogle, A. (2019, July 10). *Encryption laws developed after little consultation with Australian tech companies, FOI documents reveal*. Retrieved from ABC News: https://www.abc.net.au/news/science/2019-07-10/dutton-encryption-laws-australian-tech-sector-not-consulted-foi/11283864

Brown, E. (2018, October 25). *Most consumers have cyber security concerns, but a fraction take action*. Retrieved from ZDNet: https://www.zdnet.com/article/most-consumers-have-cyber-security-concerns-but-a-fraction-take-action/

Clarke, M. (2018, Oct 19). *Metadata laws under fire as 'authority creep' has more agencies accessing your information*. Retrieved from ABC News: https://www.abc.net.au/news/2018-10-19/authority-creep-has-more-agencies-accessing-your-metadata/10398348

Douglas, D. (2014, May 05). *Target CEO resigns after massive data breach*. Retrieved from Washington Post: https://www.washingtonpost.com/business/economy/target-ceo-resigns-after-massive-data-breach/2014/05/05/ef6cbee2-d457-11e3-8a78-8fe50322a72c_story.html#targetText=Target's%20president%20and%20chief%20executive,massive%20data%20breach%20last%20year.&target

KPMG. (2019, April 17). *Consumer Loss Barometer - The economics of trust*. Retrieved from KPMG: https://home.kpmg/au/en/home/insights/2019/03/trust-in-the-time-of-disruption.html

Mallis, A. (2019, August 6). Waves Of Regulation Are Complicating Cybersecurity Strategy For Australian Organisations, Says AustCyber CEO. *Which-50*, p. 1. Retrieved from https://which-50.com/waves-of-regulation-are-complicating-cybersecurity-strategy-for-australian-organisations-says-austcyber-ceo/

Manuel, D. (2019, February 28). *Seven ways the government can make Australians safer – without compromising online privacy*. Retrieved from The Conversation: https://theconversation.com/seven-ways-the- government-can-make-australians-safer-without-compromising-online- privacy-111091

Otarris. (2019, April 10). Are you ready to manage all that. McLean, VA, USA. Retrieved from Otarris - On Trend: 20.4 Billion IoT Devices by 2020: https://www.otarris.com/on-trend-20-4-billion-iot-devices-by-

2020/#targetText=Gartner%20forecasts%20that%2020.4%20billion,%243%20trillion%20annually%20by%202026.

Pearce, R. (2019, July 08). *Australia's 'encryption' law could erode consumer trust in tech: Amazon*. Retrieved from Computerworld: https://www.computerworld.com.au/article/663754/australia-encryption-law-could-erode-consumer-trust-tech-amazon/

Pearce, R. (2019, August 01). *Cyber security: Sorting through Australia's 'train smash of a legislative landscape'*. Retrieved from Computerworld IDG: https://www.computerworld.com.au/article/664844/cyber-security-sorting-through-australia-train-smash-legislative-landscape/

Pearce, R. (2019, July 5). *Government acknowledges Aussie businesses have taken hit from 'encryption' law*. Retrieved from Computerworld: https://www.computerworld.com.au/article/663711/government-acknowledges-aussie-business-taken-hit-from-encryption-law/

Reichert, C. (2018, March 29). *Government passes critical infrastructure national security Bill*. Retrieved from ZDNet: https://www.zdnet.com/article/government-passes-critical-infrastructure-national-security-bill/

Rutter, D., & Khan, G. (2019, Jun 05). *How to fix the government trust issue*. Retrieved from PWC Digital Puls: https://www.digitalpulse.pwc.com.au/citizen-government-trust-experience/

Schwartz, M. (2018, June 28). *Cybercrime Groups and Nation-State Attackers Blur Together*. Retrieved from Bankinfosecurity: https://www.bankinfosecurity.com/cybercrime-groups-nation-state-attackers-blur-together-a-11141

Telstra. (2019). *Telstra Security Report 2019.* Melbourne: Telstra.

van den Berg, B., & Keymolen, E. (2017, March 19). Regulating security on the Internet: control versus trust. *International Review of Law, Computers and Technology, 31*(2), pp. 188-205.

Verizon. (2019). *2019 Data Breach Investigaions.* New York: Verizon.

WEF. (2019, February 25). *International law cannot keep up with cyber-criminals*. Retrieved from WEF Cybersecurity: https://www.weforum.org/agenda/2019/02/why-international-law-is-failing-to-keep-pace-with-technology-in-preventing-cyber-attacks/

APPENDIX 1

Traffic Light Protocol

Code	FS-ISAC Rating	FS-ISAC Interpretation
RED	Sources may use FS-ISAC RED when the information's audience must be tightly controlled, because misuse of the information could lead to impacts on a party's privacy, reputation or operations. The source must specify a target audience to which distribution is restricted.	Recipients may not share FS-ISAC RED information with any parties outside of the original recipients.
AMBER	Sources may use FS-ISAC AMBER when information requires support to be effectively acted upon, but carries risk to privacy, reputation or operations if shared outside of the organisation's involved.	Recipients may only share FS-ISAC AMBER information with other FS-ISAC members, staff in their own organisation who need to know or with service providers to mitigate risks to the member's organisation if the providers are contractually obligated to protect the confidentiality of the information. FS-ISAC AMBER information can be shared with those parties specified above only as widely as necessary to act on the information.
GREEN	Sources may use FS-ISAC Green when information is useful for the awareness of all participating organizations as well as with peers within the broader community.	Recipients may share FS-ISAC GREEN information with peers, trusted government and critical infrastructure partner organisations, and service providers with whom they have a contractual relationship, but not via publicly accessible channels.
WHITE	Sources may use FS-ISAC WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	FS-ISAC WHITE information may be distributed without restriction, subject to copyright controls.