RECOMMENDATION PAPER FOR AUSTRALIA'S NATIONAL CYBER SECURITY STRATEGY 2021

AUGUST 2021

SEKAR LANGIT
CYBER SECURITY ANALYST
INTERNET 2.0

1. INTRODUCTION

Cyber security has become increasingly important with the rise of the internet-capable devices and the Internet of Things (IoT). In 2018, Schneider Electric's Smart Home Spaces estimated that the average Australian household has 17 connected devices, including smartphones, tablets, smart watches, smart TVs, fitness trackers, and virtual assistant devices such as Google Home and Amazon's Alexa. Australian society has also seen broad uptake of social media. Research by JWS Research commissioned by Australian Cyber Security Centre (ACSC) in September 2020 found that seven in ten Australians use Facebook, and almost half use YouTube or Messenger. These factors are vectors for cyber security vulnerability.

Unfortunately, the significant increase in internet usage is not followed by better understanding of risks and security measures in the community. As of 2020, only 17% of Australians considered as having high awareness of cyber security and are actively implementing security measures, while 34% of Australians are in high risk with little to no implementation of online safety measures.[1] Half of Australian population is eager to learn more about cyber security,[1] which demonstrates a willingness in the community to improve cyber security capabilities.

Filling in this gap is critical. By some estimates, cyber security incidents cost Australians and Australian businesses billion of dollars every year. For Australian businesses, the cost of cyber security incidents is estimated to be $29 billion per

[1] Cyber Security Research Report, Prepared for Australian Signal Directorate, September 2020, by JWS Research (*https://www.cyber.gov.au/sites/default/files/2020-12/ASD%20Cyber%20Security%20Research%20Report.pdf*)

year – equivalent to 1.9% of the entire country's GDP.[2] For individuals, the approximate cost is $316 million annually, noting that there are many cases left unreported.

Australians' lack of cyber security knowledge was highlighted recently in Microsoft's Global Tech Survey 2021, which reported that Australia ranks number 2 globally on the list of countries that are most vulnerable to remote access scams. Data from IDCARE (a government-funded organisation that provides support for cyber security incidents) shows that during a two-week period in June 2021, their case managers were involved in nearly 1000 cases of remote access scams, resulting in an overall financial loss of over $1.83 million. ACSC has reported that they received 59,806 cybercrime reports during 2019-2020, or the equivalent of one complaint in every 10 minutes.[3]

"Over the period of 1 July 2019 to 30 June 2020, ACSC responded to 2,266 cyber security incidents and received 59,806 cybercrime reports at an average of 164 cybercrime reports per day, or one report every 10 minutes."- ACSC

The Australian Government, through the National Cyber Security Strategy 2020, has identified groups with particular vulnerability to cyber incidents; those who are not familiar with technology, older people, and those with limited English language

[2] Direct costs associated with cybersecurity incidents costs Australian businesses $29 billion per annum (*https://news.microsoft.com/en-au/features/direct-costs-associated-with-cybersecurity-incidents-costs-australian-businesses-29-billion-per-annum/*)

[3] ACSC Annual Cyber Threat Report 2019-2020 (*https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf*)

capabilities. When it comes to businesses, Small and Medium Enterprises (SMEs) tend to be the most vulnerable to cyber incidents.

This paper identifies several cybersecurity vulnerabilities in the Australian community and suggests potential steps the government can take, supplementary to the Cybersecurity Strategy. It explores various ways to strengthen Australian government's cyber security engagement in the community and provides best practices to create a more secure cyberspace for Australians, by putting the vulnerable victims at the heart of the strategies.

2. CURRENT CYBER SECURITY ENVIRONMENT – ISSUES

2.1. Lack of Basic Understanding of Cyber Security Hygiene

The majority of successful cyber attacks have a contributing human factor. 34% of Australian population are at high risk of cybercrime with little to no awareness and implementation of cyber security measures. Consequently, Australians are one of the most targeted populations for cyber-attacks globally. Among the vulnerable victims of cyber incidents in Australia are those who are not familiar with technology, older people, and those with limited English language capabilities.

Australian Cyber Security Centre (ACSC) has been in the forefront of Australian government's cyber security engagement with both businesses and the general public. It has created several campaigns to spread awareness of cyber security

best practices, such as Stay Smart Online and the most recently launched program; Act Now Stay Secure. Through the Act Now Stay Secure campaign, ACSC produces a number of materials on basic cyber security hygiene, including documentations on how to set up multi-factor authentication, a guide on creating strong passwords, how to shop online securely, and the importance of keeping devices updated.

Figure 1. One of ACSC's resources as part of Act Now Stay Secure Campaign

Source: ACSC (cyber.gov.au)

Figure 1 shows the example of documentation that ACSC produced as part of the Act Now Stay Secure campaign.

While these resources are important for strengthening the community's cyber security hygiene, their impact are limited by limited public awareness of ACSC itself. Only 19% of Australia's population is aware of ACSC, and "not knowing

where to report" is still the second highest reason for unreported cases despite ACSC providing 24/7 cyber hotline[4].

Secondly, the ACSC's resources are contain jargon such as malicious and malware, which makes cyber security hygiene sounds more complicated than it should be and can be inaccessible to the three special vulnerability groups. If the aim is to strengthen basic online safety measures and in particular to develop basic cyber security hygiene amongst vulnerable groups, the language used in ACSC resources needs to be simplified and their accessibility prioritised.

Furthermore, as shown on one of ACSC's poster on figure 2, ACSC's cyber security campaign is predominantly based on fear. For instance, the wordings "Keep Cybercriminals Out" or "Technology Advances Rapidly. So Do Cybercriminals" along with dark background colour on the posters. This is counter-productive and not conducive to developing a culture of learning about cyber security.

[4] Cyber Security Research Report, Prepared for Australian Signal Directorate, September 2020, by JWS Research (*https://www.cyber.gov.au/sites/default/files/2020-12/ASD%20Cyber%20Security%20Research%20Report.pdf*)

Figure 2. One of ACSC's poster as part of Act Now Stay Secure campaign

Source: ACSC (cyber.gov.au)

Lastly, despite the Australian government recognising people with limited English language capabilities as one of the most vulnerable groups to cyber incidents, there is no translated content on ACSC website at the date of writing, as shown in figure 3 below.

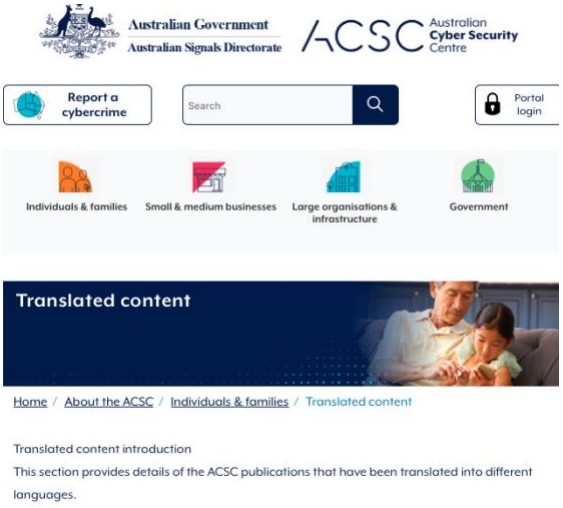

Figure 3. No translated resources on ACSC website

Source: ACSC (cyber.gov.au)

2.2. Cyberspace is a Scary World

ACSC reported that they received 59,806 cybercrime reports during 2019-2020 or, or the equivalent of one complaint in every 10 minutes. The most common type of cybercrime in Australia is malicious email (phishing and spearphishing), often impersonating the Australian government.

One case study that took place in 2018 was an email that circulated in the community pretending to be myGov, a government platform that connects various government services, including Medicare and tax services. At a first glance, the email appeared to be legitimate, as shown on figure 4 below. It asked the email receiver to update their Electronic Fund Transfer (EFT) payments with Medicare.

Figure 4. Malicious email claiming to be myGov

Source: ABC

Upon clicking the link, it would take the receiver to a clone website that look very identical to myGov website, with slightly different URL: www[dot]mygovau[dot]net, instead of my.gov.au.

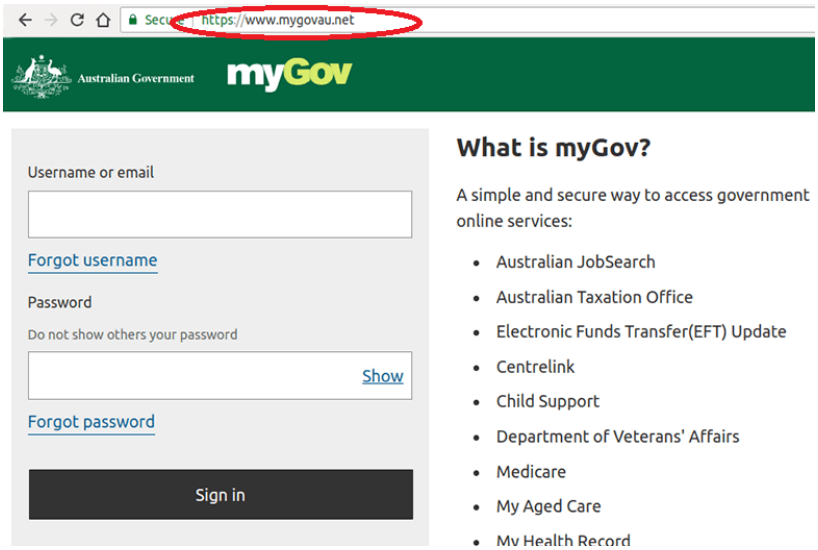

Figure 5. Clone website of myGov

Source: ABC

The clone website asked for victim's myGov credentials, along with secret security question and answer, as well as bank account details. This type of threat continues to impact the community, and similar malicious emails still regularly circulate in the community.

The second biggest threat faced by Australians in the cyberspace is ransomware, where the threat actor locks up or encrypts victim's computer or files and demands a ransom payment. This type of attack mainly targets private sector organisations. While some major companies still have vulnerabilities in their cyber defences and can become targets, SMEs are targeted frequently by criminals since they typically invest less in cyber security.

2.3. Security is not a Priority

Despite widespread uptake of IoT and internet-capable devices in Australia, there is yet to be clear standards on cyber security measures for digital product development. As the result, majority of IoT products are vulnerable to cyber threat and data breach.

The Australian Government also needs to vigilant in implementing cyber security standard and practises. ACSC's Threat Report indicated that Commonwealth and State/Territory governments rank number one and two on the most affected sectors during 1 July 2019 to 30 June 2020. While ACSC admitted that the high number was partly due to the close relationship between ACSC and the government which leads to more compliance in reporting cyber security incidents, the number of incidents reported in both Commonwealth and State/Territory governments, 436 and 367 incidents respectively, are still extremely high. Considering the amount of public data that the government holds, a significant change in approaching cyber security defence and overall cyber security hygiene is much needed.

3. FUTURE CYBER SECURITY STRATEGIES - RECOMMENDATIONS

3.1. Communicating Cyber

Basic cyber security education is fundamental in getting the nation ready for myriad of threats in this digital world. For general public, cyber security resources can appear as too complicated and intimidating, therefore simplifying terminology is essential to make sure that the actual message is not lost in the jungle of information and ensuring that documents are accessible.

As an example of best practice in this regard, the Australian Communications and Media Authority (ACMA) produces a number of straightforward educational resources regarding phone scams.

Figure 6. ACMA's phone scam educational resources

Source: ACMA Website

The educational resources are also available in Simplified Chinese, Traditional Chinese, Arabic, Vietnamese, and Italian. Translated contents for resources containing important issues such as cyber security make a significant difference since non-English speaking Australians are among those most vulnerable to cyber security incidents.

Figure 7. ACMA's translated content

Source: ACMA Website

Another great example is from the UK's equivalent of ACSC – National Cyber Security Centre (NCSC). NCSC creates thematic campaign in accordance with the time of the year and the most threat circulating in the community at present. For instance, NCSC launched CyberAware campaign in December 2020

by running TV, radio, and online media advertisement about doing online shopping securely.

Figure 8. CyberAware campaign from UK's NCSC

Source: NCSC

The use of multiple broadcasting media in this campaign provides a higher opportunity that the message will be delivered to the whole community. It is also a good way to build awareness about NCSC, therefore making sure that NCSC will be in the forefront of the community's minds when seeking information or support on cyber security.

These practices could be readily adopted by the ACSC to support its cyber security awareness activities.

3.2. Building a More Secure Cyberspace for Australians

3.2.1. DNS Filtering

DNS filtering is the practice of preventing access to malicious websites. If a website has been deemed a threat, its IP address can

be blocked using a DNS filter and consequently access to it is prevented. When done effectively, DNS filtering can shorten the life cycles of malicious websites in the cyberspace and therefore preventing more people to fall victim. A continuous share of information among individuals, public sector, and private sector is important in building a sustainable DNS filtering system.

UK's NCSC launched an effective system to feed in to DNS filtering system called SERS (Suspicious Email Reporting Service). Using SERS, organisations can add a button on their Microsoft 365 accounts to report suspicious emails directly to NCSC.

"Since its launch in April 2020, the Suspicious Email Reporting Service has received over 6,500,000 reports from the public – resulting in the removal of more than 97,000 scam URLs."- NCSC

Australia will benefit from making a system like SERS available to use by companies and general public. This system will simplify incident reporting and thus will make it easier for the public to report suspicious emails that may include malicious links.

Currently in the UK, SERS has enabled NCSC to completely remove malicious URLs in reported phishing emails in only four hours.

3.2.2. Security Labelling for IoT Products

Security should be in the forefront of digital product development. Currently, there is no enforcement of this concept in Australia,

putting Australians at risk of cyber attacks targeting their multiple household or personal smart devices. One example is the 2016 Mirai botnet attack in the US targeted IoT devices such as home routers and IP cameras. The attack resulted in key global internet services inaccessible in the US East Coast.

Ultimately, a clear mandatory security standard for smart devices is of paramount importance to guide industry in creating a built-in security for IoT devices in Australia. In addition to that, a mandatory security labelling such as Singapore's Cybersecurity Labelling Scheme (CLS) will provide more incentive for industry to build the best security for their products, as well as enabling consumers to make security-aware purchases.

Furthermore, cyber security labelling could also incentivise industries to report cyber incidents without the fear of losing market share, since their efforts to improve their level of security defence will not be left unrecognised.

3.2.3. Enforcing Better Cyber Defence for Public Data Holders

During 1 July 2019 to 30 June 2020, the Commonwealth and State/Territory governments recorded the most cyber security incidents among other sectors in Australia. This is a great concern considering the amount of public data that the government holds.

Threat actors are actively collecting vulnerabilities of their possible victims and the technology that they are using during this reconnaissance stage is increasingly effective. Therefore, public data holders, from the government to large businesses and SMEs, should be subject to a more rigorous cyber defence standard.

Cyber defence standards for public data holders should not only refer to their staff's cyber hygiene, but also to being open about what kinds of data that they hold, how long they keep data in their systems, what the procedure requesting removal of personal data is, and most importantly a clear standard for security systems for public data holders' data centres.

4. CONCLUSION

Cyber security has increasingly been an important issue in the digital world. The Australian government has identified three groups of heightened vulnerability to cyber incidents: those who are not familiar with technology, older people, and those with limited English language capabilities. However, the current national cyber security strategy has not fully centralised these vulnerable groups.

The paper provides several recommendations, including:

- Simplifying cyber security communications to the public by using straightforward language and utilising multiple broadcasting media for delivery;

- Implementing an accessible cyber incident reporting system that will enable a national DNS filtering system more effectively, and thus limiting the life cycle of threats;
- Implementing mandatory security labelling for digital products, and;
- Enforcing more rigorous cyber defence systems for public data holders.

REFERENCES

1. Australia's Cyber Security Strategy 2020 (*https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf*)

2. United Kingdom's National Cyber Security Strategy 2016-2021 (*https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021)*

3. Cyber Security Research Report, Prepared for Australian Signal Directorate, September 2020, by JWS Research *(https://www.cyber.gov.au/sites/default/files/2020-12/ASD%20Cyber%20Security%20Research%20Report.pdf*)

4. Cyber Security is a Foreign Language (*https://contentsecurity.com.au/cyber-security-is-like-a-foreign-language/)*

5. ACSC's Translated Content (*https://www.cyber.gov.au/acsc/individuals-and-families/translated-content)*

6. Average Australian Home has 17 Connected Devices (*https://www.smh.com.au/business/consumer-affairs/the-average-aussie-home-has-27-connected-devices-here-s-why-that-s-growing-20181012-p509bw.html*)

7. Why are Australians More Vulnerable to Tech Support Scams? – iDcare's Newsletter 26 July 2021 *(https://www.idcare.org/latest-news/why-are-australians-more-vulnerable-to-tech-support-scams*)

8. ACSC Annual Cyber Threat Report 2019-2020 (*https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf*)

9. Direct costs associated with cybersecurity incidents costs Australian businesses $29 billion per annum (*https://news.microsoft.com/en-au/features/direct-costs-associated-with-cybersecurity-incidents-costs-australian-businesses-29-billion-per-annum/*)

10. Microsoft Security Intelligence Report (*https://clouddamcdnprodep.azureedge.net/gdc/gdcNWFXmR/original*)

11. ACMA's Phone Scam Educational Resources (*https://www.acma.gov.au/phone-scam-educational-resources*)

12. ACSC's IoT Code of Practice: Guidance for Manufacturers (*https://www.cyber.gov.au/acsc/view-all-content/publications/iot-code-practice-guidance-manufacturers*)

13. myGov Scam Tricking Victims into Handing Over Bank Details through Cloned Website (*https://www.abc.net.au/news/2018-07-05/mygov-scam-clones-government-website-medicare-phishing-email/9942908*)

14. Beware of New myGov Identity Scam (*https://www.servicesaustralia.gov.au/individuals/news/beware-new-mygov-identity-scam*)

15. What is DNS Filtering? (*https://www.webroot.com/au/en/resources/glossary/what-is-dns-filtering*)

16. What is DNS Based Web Filtering? (*https://www.hipaajournal.com/what-is-dns-based-web-filtering/*)

17. ETSI's Cyber Security for Consumer Internet of Things: Baseline Requirements (*https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf*)

18. Govt Unveils IoT Code of Practice to Protect Devices from Hacking (*https://www.itnews.com.au/news/govt-unveils-iot-code-of-practice-to-protect-devices-from-hacking-552802*)

19. Code of Practice: Securing the Internet of Things for Consumers (*https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf*)

20. Strengthening Australia's Cyber Security Regulations and Incentives (*https://www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australia-cyber-security-regulations-discussion-paper.pdf*)

21. Cyber-warning for Festive Shoppers (*https://www.bbc.com/news/technology-55171454)*

22. Email Innovation Simplifies Takedown of Cyber Scams (*https://www.bbc.com/news/technology-55171454)*

23. Singapore's Cyber Security Labelling Scheme (*https://www.csa.gov.sg/Programmes/cybersecurity-labelling/about-cls*)