EasyChair Preprint

№ 5822

Australian Cybersecurity Landscape - What Is Australia's Capability Against the Growing Sophistication of Cyber Threat Actors?

Aljim Labilles

June 16, 2021

Australian Cybersecurity Landscape

What Is Australia's Capability Against the Growing Sophistication of Cyber Threat Actors?

Aljim O Labilles
COMP1102 Fundamentals of Computational Intelligence
Flinders University, South Australia

labi0008@flinders.edu.au

Abstract

The continued advancement in Information Technology comes hand-in-hand with the need for Information Security. Globally, a recent trend in the increase of frequency and sophistication of the ways cybercriminals conduct their attacks has been observed. Australians are not immune to the activities of cyber threat actors and the adequacy of Australia's capability in defending its sovereign interest against such attacks needs a constant looking into to develop strategies and policies of resilience towards cyber vulnerabilities.

1 Introduction

One of the great highlights of the 2020 COVID-19 pandemic, is the growth in accessing cloud-based resources. While we move more services online, we tend to neglect to see the security implications it brings when we move these services online. "*Cybercriminals are developing and boosting their attacks at an alarming pace…*" (Stock, 2020), this is true in Australia as it is globally. Australia's cybersecurity capabilities need to be scrutinized to find out if we are at par with other western nations. The current Cybercrime Act 2001 needs to be looked at, and be checked if it still addresses the new categories of threat-actors and their attack vectors and strategies.

This research study aims to ascertain the current landscape of Australia's Information Security ('**infosec**') and the defensive capabilities Australia currently use to combat known and anonymous cyber threat actors. This study will, in general terms, also state the action that Australia has taken in recent time to address its cyber defence.

2 History of Australian Infosec

The first federally recognized infosec strategy came out in the year 2000 which was included in the *Defence 2000: Our Future Defence Force*, it was followed the year after by the *E-Security Initiative.* On 2 July 2008, Australia announced the review of the *E-Security Initiative* that was made in 2001 which led to the *Cyber Security Strategy ('**CSS')*** which was released in November 2009. The CSS featured two initiatives: the *Computer Emergency Response Team ('**CERT** Australia')*, which commenced operating in January 2010, and the *Cyber Security Operations Centre ('**CSOC')*** which was also launched in January 2010 (Brangwin, 2013). In 2014, the CSOC then became the *Australian Cyber Security Centre ('**ACSC**')*.

Since then, no bigger stride in the infosec industry has been made other than the release of the *Australian Cyber Security Strategy 2020 ('**ACSS2020**').* To further move on, we need to know what current legislations are in place to define a cybercriminal and their action, in Australia.

3 The Cyber Laws in Australia

All defence strategies need to be within the 4-corners of the written legislature. The definition of an attack must be clearly defined, to unambiguously determine if an action in the digital realm is indeed illicit or not. Also, a clear definition of the inclusions of the words "digital information" must be clearly stated. The following legislations are in-forced in Australia which pertains to cybersecurity:

3.1 Cyber Crime Act 2001

The *Cyber Crime Act 2001* (Legislation, 2001) defines the data stored in a computer, the definition of illegal access, modification or impairment of

such data, and the jurisdiction this Act envelops in its scope, amongst more information in the Act.

3.2 Privacy Act 1988

The *Privacy Act 1988* (2020) legislates the use of personal information. This piece of legislation does not pertain to any specific cybersecurity practice. However, an illicit cybersecurity action that discloses personal information could lead to the violation of the Office of the Australian Information Commissioner (2012) which is defined by the *Privacy Act 1988*.

3.3 Spam Act 2003

The *Spam Act 2003* was legislated by the Australian Parliament back in 2003 to:

- Regulate commercial email and other types of commercial electronic messages.
- Commercial electronic messages must include information about the individual or organisation that authorised the sending of the message.
- Commercial electronic messages must have a working unsubscribe option.
- Address-harvesting supply, acquisition and use are illegal.

3.4 Security of Critical Infrastructure Act 2018

"This Act creates a framework for managing risks to national security relating to critical infrastructure" (Legislation, 2018).

3.5 Telecommunications (Interception and Access) Act 1979

The *Telecommunications (Interception and Access) Act 1979* states that it is illegal for an individual to access private telecommunications without the consent of the parties involved in that communication (Legislation, 1979).

3.6 The Australian Privacy Principles

The *Australian Privacy Principles* gives an organisation or agency control over their handling practices of information according to their business models and the needs of each individual (Office of the Australian Information Commissioner, 2014).

4 The Increased Cyber Security Threat

Globally, all nations are experiencing a rapid increase in information technology (Kaur & KR, 2021). This rapid increase in information technology is proportional to the increase of cyberattacks or actors with malicious intent. Due to the sophistication and increase of cybersecurity threats, many academic believe and move to educate the current population about the risk and consequences of cyber-security (Rowe et al., 2011). The following enumerates various types of cyberattack commonly used in today's cyber landscape (Kaur & KR, 2021):

4.1 Cryptographic Attack

Type of attack in which the threat actor tries to circumvent the cryptography of the system to find a weakness in the cryptographic protocol, cipher, or code without the authorized key. This attack is also known as "cryptanalysis attack".

4.2 Access Attack

Type of attack in which the threat actor tries to access the victim's machine from which they have no authority to use with the malicious intent of manipulating the available data for the threat actor's benefit. An example of this is the perpetrator accessing the email server illegally without the consent of the individual who owns the email data.

4.3 Reconnaissance Attack

Type of attack in which the threat actor scans the victim's digital and/or physical infrastructure while gathering information which will be used for another escalated form of attack at a later time. https://hunter.io/ is a commonly used tool for email reconnaissance by ethical hackers.

4.4 Active Attack

Type of attack in which the threat actor actively intercepts the data and manipulating its content before it reaches the intended destination. This attack type is also known as "Man-in-the-Middle Attack".

4.5 Passive Attack

Type of attack in which with an inherent similarity with a reconnaissance attack where a threat actor accesses the information shared through transmission with the threat actor's main aim is to gather important information which can be used illegally at another time.

4.6 Phishing Attack

Type of attack in which the threat actor preys on the gullibility of the victim to trust a malicious email from the threat actor posing as a legitimated electronic message from a reputable source to access important and confidential information such as usernames, login passwords, credit card numbers, PINs, etc.

4.7 Malware Attack

Type of attack in which the threat actor executes malicious software ("mal-ware") without the permission of the victim to take control or collect information on the victim's machine. A phishing attack is the most common attack vector of this type of cyberattack.

4.8 Attack on Quantum Key Distribution

"An attack has done while transmitting any data through a quantum channel either by forge a single photon, multiple photons, or by time elapsing of pulses" (Kaur & KR, 2021)

5 Australia's New Cyber Security Strategy

The digital information landscape transformation has developed relatively fast in the last 15 years and even by that statement the recent speed of change seems exceptional during the period of the global pandemic. The launch of a new national cybersecurity strategy, partnered with an increase in financial commitments by the federal government, shows that Australia has come to a point where the risks and consequences posed by a mediocre cybersecurity scheme are significantly higher even compared to a global pandemic such as the COVID-19 (ASPICanberra, 2020).

The $1.67 billion investment over 10 years includes:

- Security of critical infrastructure that Australians rely on.
- Innovative and up to date ways to identify and mitigate cybercrime.
- Improve the cybersecurity defences of government networks and data.
- Improve collaboration.
- Increased awareness.
- Partnerships with the private sector through the Joint Cyber Security Centre program.
- Framework for small businesses and medium enterprises for their cyber resilience.
- Improvement in securing the Internet of Things (IoT) devices.

This strategy is envisioned to be delivered through direct and indirect initiatives of the government, businesses and the community (Department of Home Affairs, 2020).

Conclusions

With billions of people using the internet in 2021, the amount of information being transmitted has exceeded 2.5 quintillion bytes per day (Alani, 2021). This rapid growth in the creation of data has pushed the use of digital information to different platforms which demand 'infosec'. The new *Australia's Cyber Security Strategy 2020* aims to address Australia's defences against cybercriminals and protect its people from damages typically brought on as a consequence of these cybersecurity breaches. The adequacy of a defensive landscape can in this setting, never be quantified or stated as sufficient, due to the rapid increase of sophistication in cybersecurity attacks. Australia's continued persistence in information security shows that while we combat an ever-growing array of cybercriminals, Australia's defensive strategies and policies needs continued and constant periodic review and redevelopment to increase Australia's capability and resilience towards cybercriminal's malicious activities.

As the methods of attack is evolving daily in the cyber world, a static approach on defence will not be enough against cyber threat. Cyber defence must evolve and develop together with the growing vulnerability and the sophisticated method it carries with it.

References

Alani, M. M. (2021). Big data in cybersecurity: a survey of applications and future trends. *Journal of Reliable Intelligent Environments*, 1-30.

ASPICanberra. (2020). *Australia's Cyber Security Strategy In-Focus*.

Brangwin, N. (2013). *Cyber security*. Parliament of Australia. Retrieved 10 March from https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BriefingBook44p/Cyber

Department of Home Affairs. (2020). *Australia's Cyber Security Strategy 2020*. Retrieved 5 March from https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf

Kaur, J., & KR, R. K. (2021). The Recent Trends in CyberSecurity: A Review. *Journal of King Saud University-Computer and Information Sciences*.

Telecommunications (Interception and Access) Act, (1979).

Cybercrime Act 2001, (2001).

Spam Act, (2003).

Security of Critical Infrastructure Act, (2018).

Office of the Australian Information Commissioner. (2012). *The Australian Privacy Principles*. Retrieved 05 March from https://www.oaic.gov.au/privacy/australian-privacy-principles/

Office of the Australian Information Commissioner. (2014). *Australian Privacy Principles*. Retrieved 05 March from https://www.oaic.gov.au/privacy/australian-privacy-principles/#:~:text=The%20Australian%20Privacy%20Principles%20are,to%20adapt%20to%20changing%20technologies.

Rowe, D. C., Lunt, B. M., & Ekstrom, J. J. (2011). The role of cyber-security in information technology education. Proceedings of the 2011 conference on Information technology education,

Stock, J. (2020). *INTERPOL report shows alarming rate of cyberattacks during COVID-19*. Interpol. Retrieved 08 March from

A Copyright