Challenges faced by Australian Law Enforcement in investigating and prosecuting Cyber crimes.

Author : Mohammed Sadiq Abuwala

Student ID : 45921407

INTRODUCTION

The digital landscape is continuously growing. As digital connectivity increases, many operations are becoming digitized. Some examples of these are voting, bank transactions, and language translation. Additionally, newer technologies such as Internet of Things (IoT), social media platforms, and online learning tools offer further avenues for criminals to exploit. This exploitation has far reaching consequences because criminals are using the digital landscape to conduct a large variety of crimes such as terrorism, human trafficking, drug trafficking, and child sexual abuse. Law enforcement agencies should be well positioned to harness these technologies and tackle these challenges as they arise. This paper explores the challenges faced by Australian law enforcement in investigating and prosecuting cyber crimes in such a constantly changing landscape.

1. WHAT IS CYBERCRIME?

In Australia, cybercrime is defined as:

- ➔ " Crimes directed at computers or other information communications technologies (ICTs) (such as computer intrusions and denial of services attacks).
- ➔ Crimes where computers or ICTs are an integral part of an offence (such as online fraud) " (Cybercrime and identity security, 2020) .

2. THE DIGITAL ENVIRONMENT

2.1. RAPID GROWTH

Our lives are rapidly being transformed by the internet and digital technologies. Today, they are used to conduct business operations, social interactions, access data, and engage with government. The number of users with access to these technologies is also increasing as they become more consumer friendly (i.e affordable, and widely available). The figure below shows the number of individuals (% of population) in Australia using the internet (Individuals using the Internet (% of population) - Australia | Data, 2019):

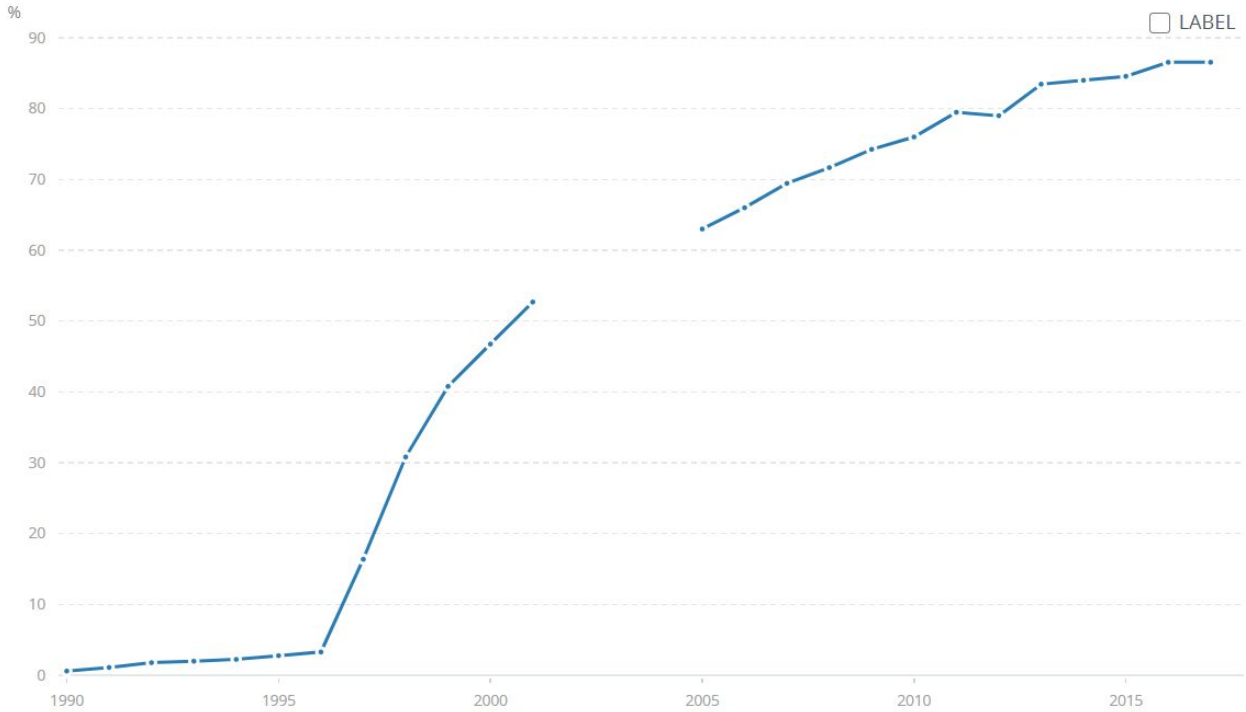

Figure 1 : % of Australian population using the internet from 1990 - 2017

The statistics shown in the graph above is the latest official release by The World Bank. Its key findings are noted below:

- ➔ In the year 1990, 0.585% of the population had access to the internet.
- ➔ By the year 2017, 86.545% of the population had access to the internet.

Traditionally, the internet was accessed on computers or laptops. In 1999, NTT DoCoMo released the first consumer based mobile browser based internet service. Over the years, The advancement in technology has also led to consumers now having a wide variety of devices to choose from with which to access the internet. This reasoning is more clear when we study the most recent official statistics released by the Australian Bureau of Statistics. The table below shows the devices used to connect to the internet by household from 2014 - 2015 and 2016-17 (Australian Bureau of Statistics, 2018):

	2014-15 (%)	2016-17 (%)
Internet connected games console	25.1	26.7
Internet connected music/video player	26.1	18.6
Internet connected TV	26.8	42.1
Tablet	61.9	66.4
Mobile or smart phone	86.0	91.0
Desktop or laptop computer	93.6	91.4

Figure 2 : Devices used to access the internet from 2014-2015 and 2016-2017

The above table establishes some key findings:

- ➔ A large variety of devices are used by Australian consumers today to access the internet.

- ➔ While some devices have seen a decline in use (For example: Internet connected music / video player), other devices have seen a rapid rise in usage (For example: Internet connected TV). Hence, this validates the argument that Australia is seeing a rapid intake of technology and growth in digital connectivity.

2.1. CONSEQUENCES OF RAPID GROWTH

Better access, dependency, and openness also introduces greater risks. It has created new opportunities for cybercriminals who seek to target the vulnerable members in our

community. Cybercriminals are using the increased digital connectivity and technological innovations to commit a large variety of crimes. This trend can be noted in the annual cyber threat report released by the ASCS for the period of 2019 - 2020. These findings can be viewed in the pie chart below (Australian Cyber Security Center, 2020):

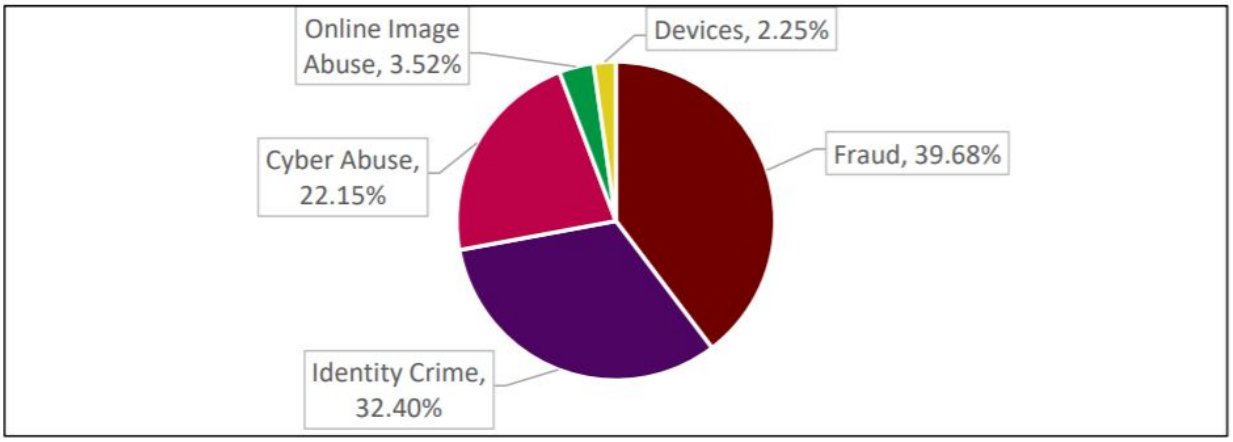

Figure 3: Common types of cybercrime reported in Australia for the year 2019 - 2020

The above figure shows that the most common category of cybercrimes reported are Fraud. It refers to any crime that uses criminal deception for the purpose of personal or monetary gain. Some examples of such crimes are romance and shopping scams. Identity crimes are the second most committed cybercrimes. It relates to the misuse of personal information for personal or monetary gain.

Cybercriminals are also taking advantage of increased digital connectivity and technological innovations to commit new and sophisticated cyberattacks. In contrast, consumers are more focused towards the operation of these technologies and are not necessarily focused towards cybersecurity. This trend can be noted as key findings in the survey results on Small to Medium Businesses (Australian Cyber Security Centre, 2020):

- ➔ 1 in 5 SMBs that responded to the survey were not aware of the term ‘phishing’.
- ➔ Almost half of SMBs reported their knowledge of cybersecurity as average or below average.
- ➔ Due to inadequate knowledge on cybersecurity, approximately half of SMBs reported investing inadequately (i.e. 500 Australian Dollars or less) to implement cybersecurity measures yearly.

Furthermore, cybercriminals are committing crimes which do not necessarily take place in or have a direct impact in the digital world. For example, the emergence of social

media tools have allowed drug smugglers to enhance communication within their network and better facilitate their crimes. A cyber criminal does not have to be present at the same location where the crime is being committed. These factors make cybercrime a lucrative endeavour. “The increasing demand for cyber exploits has made creation and distribution of malware and other hacking tools easier” (Rad, 2015). Commercially available tools are now also available which reduce the complexity of performing cyber attacks.

The frequency and cost of cyberattacks to Australian businesses is substantial and rising rapidly. The Australian Government’s cybersecurity strategy released for the year 2017 reported that the annual cost of cyberattacks to Australian businesses is estimated at 1 Billion Australian Dollars (Small Business Commissioner, 2017).

3. CHALLENGES FACED BY LAW ENFORCEMENT

3.1. IDENTIFYING CYBER CRIMINALS

There is no easy means to identify a user’s location and activity. “Several telecommunications gadgets such as Psiphon, The Onion Router (Tor) etc. are used to shield the identity of Internet users and communication are often routed via many servers which further compounds the possibility of cyber criminals being traced” (Ajayi, 2016).

There is no pre-requisite for a user to identify themselves in order to access the internet. A user simply requires an Internet Protocol (IP) address in order to gain access. The open access nature of the internet makes it even more difficult to identify users on the internet. From the perspective of law enforcement, proposing any legislation investigating or prosecuting cybercrime is irrelevant if they are unable to identify the cybercriminals.

3.2. JURISDICTIONAL CHALLENGES

Statistics reveal that in most cases, cybercriminals are not located in the same jurisdiction that they target. Cybercrime is often committed on a global scale.. The anonymity that the internet allows makes it harder to trace its users. Furthermore, as most cases are based in international jurisdictions, gathering evidence is complex and more time consuming. In addition to the cybercriminal being based outside Australia, the crime also involves multiple jurisdictions in many cases. For example, a cyber criminal may be based in one jurisdiction but store the proceeds of his criminal enterprise in a separate jurisdiction. Hence, law enforcement must coordinate with all

the jurisdictions involved in order to pursue such a case and this would be time consuming.The process also inadvertently becomes more expensive.

Every nation state conforms to a system of rules called laws which are enforced through social and governmental organizations. Its purpose is to regulate the behavior of the inhabitants in that territory. The definition of a law and its implications may vary in different jurisdictions and may not necessarily be similar. As a huge range of services that operate on the internet fall under international jurisdiction, investigating and prosecuting such cases becomes more complex. This is due to the lack of treaties and understanding between a majority of nations. Analyzing a report released by the Australian attorney general's department provides this trend. It reveals that Australia has bilateral extradition relationships with only 39 nations (Attorney-General's Department, 2019).

The lack of understanding or co-ordination between different nations can be a major issue for law enforcement. For example, if a local IP address of an attacker is located, law enforcement can immediately pursue a warrant to force the Internet Service Provider (ISP) to release records of the owner of the IP address. In contrast, if the IP address is based outside Australian borders, investigators can utilize ICANN's WHOIS query tool to identify the ISP associated with the IP address. Once registered information on the ISP is obtained, law enforcement would now have to coordinate with authorities based in that jurisdiction to obtain evidence. In many of these cases, the only way to gather sufficient evidence may be through law enforcement based in that jurisdiction.

3.3. LAW ENFORCEMENT CAPABILITIES

Law enforcement must possess the expertise required to harness these technologies in order to effectively combat cyber crime. This is because crimes are also becoming more specialised. Hiring staff with such expertise is expensive. The requirement of certain specialist tools to investigate such crimes add further to the cost of pursuing cyber crimes. Therefore, law enforcement must possess the funding and expertise in order to investigate and prosecute cyber crime.

There is evidence to suggest Australia has recently substantially increased their spending on cyber security. "The Australian Government's national Cyber Security Strategy released in 2016 and backed by around $230 million of funding, elevated cyber security to an issue of national importance" (Australian Government, 2016). Furthermore, in 2020, the federal government pledged the nation's largest ever

invested in cybersecurity. The pledge amounts to 1.35 Billion Australian Dollars over the next decade (Prime Minister of Australia, 2020).

However, the country still has a shortage of skilled cyber security professionals. This is not surprising because cybercrime is a young and emerging profession. A labor market research released by the Australian government revealed that in 2015, 42% of workforce advertisements relating to ICT Security Specialists remained vacant. This is not necessarily due to a failure of the government in hiring a skilled workforce. The study also reveals that there were only 1.7 suitable applications per vacancy. This is the lowest recorded number across all IT professions (Australian Bureau of Statistics, 2015). This shows that there needs to be more focus on cyber security skills in the education sector. To put it simply, skilled professionals must exist in order to hire them. In the year 2019, Australia had a shortage of upto 2,300 cybersecurity workers (The challenge: Australia needs to fill the workforce gap, remove startup barriers and strengthen research and development, 2020).

Australia is a part of Five Eyes. It is an intelligence alliance between five western nations: Australia, Canada, New Zealand, UK, and USA. This makes them a target of adversaries which oppose these nations or the alliance in any form. Due to these reasons, it is important that law enforcement have appropriate funding and a skilled workforce.

3.4. DIGITAL EVIDENCE

The complexity involved in many crimes involve evidence gathering at a highly technical level. This means presented evidence can be complex. To be admissible in court, digital evidence must also be authentic and proven without reasonable doubt. This inadvertently leads to lengthy arguments in court between law enforcement, prosecutors, stakeholders and expert witnesses.

Digital evidence is not always directly visible to the naked eye and like fingerprints, it is easily altered or destroyed. When digital evidence is processed by a skilled examiner, valuable data for a legal proceeding can be obtained. “Improper examination, review, or analysis by unqualified persons can yield inaccurate or misleading results and opinions” (The Forensic Laboratory Handbook Procedures and Practice, 2011).

It is also important to note the big data challenges faced by law enforcement organizations. The internet is rapidly growing in size and this means that law enforcement now also have more data at their disposal. The collection, analysis and exchange of such data to gather information of interest can be complex and time

consuming. A cybercrime does not have to be reported to be investigated by Australian law enforcement. Officials must have the technical abilities to seep through the large amount of data being gathered in order to detect cybercrimes. There must also be efficient guidelines on sharing acquired data between different states. To put it simply, a cybercrime cannot be investigated or prosecuted if law enforcement do not have the ability to detect them in the first place.

3.5. NEW TECHNOLOGIES INTRODUCE NEW ATTACK VECTORS

Newer technologies such as Internet of Things (IoT) introduce new attack vectors for cyber criminals to target. “Cyber criminals are increasingly using the seemingly innocuous IoT to deploy a range of devices and applications that hide the identity of the user by separating online identity from online activity. It was noted that such devices often have weak security and permit access to an individual company’s wider network” (Coyne, 2018). These devices are in general created for efficiency and automation and are not focused towards security. Some examples of cybercrimes committed where connectives devices may be involved are the cyber intrusion of medical devices, cars and refrigerators.

Cloud computing is another recent technology that allows individuals or businesses to store huge amounts of data in one location. They are popular because they save IT cost, energy cost and reduce system level complexity (Bojanova, Zhang and Voas, 2013). Many cyberattacks which were once directed towards organizations are now directed towards third party cloud providers. This is of particular concern because an organization could be based in Australia but have its data stored in the cloud which could be outside the Australian Jurisdiction. Hence attribution, in such cases such as identifying victims and damages could be a complex process.

3.6. COMMON CYBERATTACK METHODS

Phishing is the most common method used to commit cybercrimes in Australia. “Phishing is an online identity theft, which aims to steal confidential information such as username, password and online banking details from its victims” (). Ransomware is an emerging threat that has seen an exponential increase and hence noteworthy. “Ransomware refers to the branch of malware that, after infecting a computer, asks for a ransom” (Arachchilage and Love, 2014).

The reason such attacks are the most common methods used is because they can be simple to operate. For example, to conduct a ransomware attack, an adversary simply needs an encryption tool and an account which can store the proceeds of the crime.

Hence, there is not much operational complexity involved. In ransomware attacks, it is almost impossible for law enforcement to recover encrypted data without assistance from the cyber criminal because only they have access to the decryption key.

Cyber criminals are also continuously using these new methods to perform cybercrimes. This trend is evident when we analyze the COVID-19 threat report released by the Australian government. It is noteworthy how cybercriminals have quickly adapted to the increased digital connectivity and interaction during COVID-19 to perform cybercrimes. The key findings of the report for the period of March, 2020 - April, 2020 is discussed below (Australian Cyber Security Center, 2020):

- ➔ Access was disrupted to over 150 COVID-19 themed websites that were built for the purpose of conducting cyberattacks in Australia. Some of these websites even replicate the look of Australian government websites.
- ➔ Received more than 95 cybercrime reports relating to COVID-19 related online frauds.
- ➔ Adversaries are using COVID-19 themed phishing attacks to illicitly obtain user information belonging to individuals and businesses. There has also been an increase in SMS phishing scams where recipients are tricked into clicking on a malicious web link.

Law enforcement must stay aware and ahead of the curve with these rapid innovations in technology in order to detect, investigate, and prosecute such crimes.

4. CONCLUSION

Being connected to the internet is now deemed essential to both businesses and individuals. A business needs to be online and utilize the latest technology to stay competitive. Hence, digital activity in Australia is rising rapidly. This increased digital activity inadvertently introduces the possibility that more cyber crimes may be committed. Therefore, law enforcement officials must meet the challenges that arise relating to investigating and prosecuting cybercrimes. In case of cyber crimes, it is evident that identifying perpetrators, evidence gathering is time consuming and costly for Australian law enforcement because in most cases, they are based outside their jurisdiction. Furthermore, law enforcement must also train and hire more skilled professionals to deal with the nationwide skill shortage. Finally, the continuous transformational nature of digital technologies require Australian law enforcement to be proactive in staying up to date with the latest advancement in technologies.

References

Homeaffairs.gov.au. 2020. *Cybercrime And Identity Security*. [online] Available at: <https://www.homeaffairs.gov.au/about-us/our-portfolios/criminal-justice/cybercrime-identity-security> [Accessed 25 October 2020].

Data.worldbank.org. 2019. *Individuals Using The Internet (% Of Population) - Australia | Data*. [online] Available at: <https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=AU> [Accessed 25 October 2020].

Australian Bureau of Statistics, 2018. *Household Use Of Information Technology*.

Australian Cyber Security Center, 2020. *ACSC Annual Cyber Threat Report July 2019 To June 2020*. P.11.

Australian Cyber Security Centre, 2020. *Cyber Security And Australian Small Businesses*. P.5.

Rad, T., 2015. The Sword and the Shield: Hacking Tools as Offensive Weapons and Defensive Tools. *Georgetown Journal of International Affairs*, pp.123-133.

Small Business Commissioner, 2017. *Key Findings Cyber Scare*. P.2.

Ajayi, E., 2016. Challenges to enforcement of cyber-crimes laws and policy. *Journal of Internet and Information Systems*, 6(1), p.4.

Attorney-General's Department, 2019. *Australia'S Bilateral Extradition Relationships*.

Australian Government, 2016. *Australia's Cyber Security Strategy*. P.3.

Prime Minister of Australia, 2020. *NATION's LARGEST EVER INVESTMENT IN CYBER SECURITY*. [online] Available at: <https://www.pm.gov.au/media/nations-largest-ever-investment-cyber-security> [Accessed 25 October 2020].

Australian Bureau of Statistics, 2015. Labour Force, Australia.

Australian Cyber Security Growth Network. 2020. The Challenge: Australia Needs To Fill The Workforce Gap, Remove Startup Barriers And Strengthen Research And Development. [online] Available at: <https://www.austcyber.com/resources/sector-competitiveness-plan/chapter3> [Accessed 25 October 2020].

2011. The Forensic Laboratory Handbook Procedures And Practice. Totowa, NJ: Springer Science+Business Media, LLC.

Coyne, J., 2018. Committee Hansard. P.6.

Bojanova, I., Zhang, J. and Voas, J., 2013. Cloud Computing. IT Professional, 15(2), pp.12-14.

Arachchilage, N. and Love, S., 2014. Security awareness of computer users: A phishing threat avoidance perspective. Computers in Human Behavior, 38, pp.304-312.

Australian Cyber Security Center, 2020. *Threat Update COVID-19 Malicious Cyber Activity*. p.1.