# Challenges for preventing cyber crime

Summary

In the past three decades, the Internet has grown rapidly and evolved from its origins of military and academic use to become an integral part of communication infrastructure. Global communication has been transformed through the Internet as new opportunities have been delivered for service delivery, businesses and information and communication sharing. With these benefits of the Internet also comes new threats and problems, which criminals have been able to exploit (e. g. global nature and global reach, increased anonymization etc). Cybercrime refers to crimes where computers and information technologies are used as an integral part of the offence (i. e. online fraud, identity theft etc) or crimes directed at other computers and information technologies (e. g. malware, hacking etc). The perpetrators of cybercrime can include individual hackers, organised crime groups, corrupt company employers etc, and motivations include curiosity, fame, personal reasons, espionage etc. However, financial gain has been determined as the main motivator and explanation behind cybercrime due to the lucrative environment. One of the main challenges of cybercrime is anonymity for offenders. Through anonymization tools and other sophisticated means, offenders are able to stay anonymous online. To address cybercrime, the three recommendations are increased public and private sector relationships, an introduction of a central reporting portal and improvements in having cooperative and coordinated international responses.

Introduction

This report will begin by defining what cybercrime is and how Internet, computers and technology may be the target of, instrument of, or incidental to, criminal activity. Examples of each of these types of cybercrime activities will be included (e. g. hacking is target of). The report will then discuss the perpetrators of cybercrime, which includes individual hackers, organised crime groups, foreign intelligence operators and corrupt company employees. An example of the transnational involvement of perpetrators will be illustrated through the Dreamboard example. Motivations of cyber criminals will be discussed, which not only explores the main motive in financial gain, but also other motives such as fame, curiosity, personal reasons etc. Victims and the cost of cybercrime will be examined, which includes independent users, the private sector and the pubic sector. Different territorial jurisdictions, the Internets global reach and increased anonymity are challenges imposed on society by cybercrime. These challenges will be examined and discussed. A public-private partnership, central reporting panels and international cooperation will be recommended to reduce the harms of cybercrime.

Cybercrime

A three-stage classification is required to explain cybercrime. Firstly, cybercrimes can involve computer and computer networks being the target for criminal activity. This includes denial of service (DoS), hacking and malware attacks etc. Secondly, cybercrimes can involve computers, computer networks and the Internet being utilised to commit crimes. This includes fraud, child pornography, stalking, online piracy etc. Thirdly, cybercrimes can involve computers and computer networks being incidental

to the crime being committed. This includes computers and computer networks being used to communicate how crimes will be committed, who the chosen victims are etc (Fossi et al. 2009, p. 77).

Perpetrators

The perpetrators of cybercrime are varied, with some cybercrimes committed in groups as opposed to some committed independently. Perpetrators of cybercrime included organized crime groups (OCG's), foreign intelligence operators, individual hackers, corrupt or disgruntled company employees etc. A disparity exists between real world organized crime groups and those that exist online in cybercrime networks, in that cybercrime networks operate under a largely decentralized structure. This is because members of cybercrime networks are able remain both independent and anonymous. Furthermore, the high and global reach of the Internet means that cybercrime networks can have members from a wide variety of countries (The House Standing Committee on Communications, 2010). This is illustrated through dreamboard, which was a cybercrime network of members that shared and viewed photos and videos of child pornography. Successful law enforcement investigations led to the discovery and arrest of 50 members of this network, spanning over 14 countries (Broadhurst, 2014).

Motivations

The motivations for cyber criminals can include personal reasons (e. g. stalking), fame, espionage, curiosity, political reasons and cyber warfare. The main motivation behind cybercrimes, as argued by The House Standing Committee on Communications (2010) is financial gain. This can be

explained by the increasing presence and lucrativeness of the underground economy on the Internet through the dark web where groups, organisations and individuals actively participate in the buying and selling of fraudulent goods and services (Fossi et al., 2009). A market analysis of the content on the dark web will show that 62% of markets are drug and drug related chemicals (77% being illicit drugs, 18% drug-related chemicals and 5% pharmaceuticals) and 38% is other (44% fraud and counterfeit, 30% guides and tutorials, other 19%, hacking and malware 5% and 2% is firearms and explosives). If the focus was on the dark web drug market, given that it is the largest market on the dark web, the revenues on this market have doubled from 2013 to 2016 and then number of transactions has tripled during this time.

Victims

The victims of cybercrime include the public and private sector, and also independent users. The motivations behind cybercrimes on the public sector include protests, cyber espionage and financial motivation. For private sectors, cybercrimes committed include online fraud, extortion and theft of information. Independent users have a low level of security, which consequently makes them more vulnerable to specific types of cybercrimes such as scams, phishing scams, malware attacks etc, which is mainly motivated behind financial rewards (The Housing Standing Committee on Communication, 2010). 5. 3 million Australians (26% of the population) were affected between 2015-2016 by cybercrime, in comparison to 689. 4 million people globally (31% of the population) (Norton, 2016).

Costs to businesses

The largest cost of cybercrime in Australia is experienced in the private sector. 33% of businesses and companies experienced a cybercrime in 2015 (693, 053) in total. The average cost of a cyber attack to a business was $276, 323, with the most expensive cost per attack for businesses coming from cybercrimes such as denial of service ($180, 458), malicious insider ($177, 834) and malicious code ($105, 223). The average time to resolve an attack was 23 days, which would be increased to 51 days if the attack was a malicious insider, employee and contractor. The indirect costs to the businesses include business disruption (40%), information loss (29%), productivity loss (29%) and revenue loss (25%).

Territorial jurisdiction

Perpetrators of traditional crimes are limited to a specific territorial jurisdiction when committing a crime (e. g. perpetuator robbing a bank in Australia will be subject to Australian jurisdiction). This is not the case for cybercrime. Cybercrime offences can result in victims in a number of countries (Brenner & Koops 2004, p. 6). This imposes many unique challenges as the cybercrime acts carried out through numerous countries and states have varied bases and scopes in their cybercrime jurisdiction positions. Additionally there will be cross border conflicts in regards to which jurisdiction will prosecute the offender and how can prosecutions be carried out to avoid inconveniencing witnesses and creating duplications of evidence.

There are more than 3. 5 billion people and 40% of the worlds population online using the Internet (International Telecommunication Union 2016, p. 209). This creates an unprecedented pool of potential victims and offenders (Clough 2011, p. 673). The ‘ Love Bug’ virus is an example that illustrates the global reach of cybercrime and the adverse effects of different territorial jurisdictions. The ‘ Love Bug’ virus appeared on the Internet in May 2000. Within 10 days, over 45 million computers in over 20 countries were infected. The ‘ Love Bug’ virus was traced back to the Philippines, however virus dissemination was not a criminal offence at that time in the Philippines. De Guzman (the creator of the virus) could not be prosecuted in the Philippines and so under extradition treaties could not be extradited for prosecution to the United States or other countries where the virus inflicted damage (Brenner & Koops 2004, pp. 6-7).

Anonymity

In traditional crimes, perpetrators have a known identity and undergo a process to increase their anonymity. In cybercrime perpetrators have no identity as the Internet is ostensibly anonymous, and the application of technical anonymization procedures further increases anonymity (Lusthaus, 2012, p. 80). Cyber criminals are able to stay anonymous online through the use of anonymization tools (e. g. remailers, torrent networks etc) and other sophisticated means (e. g. spoofed IP addresses, proxy servers etc) (Clough 2011, p. 673). Iqbal et al (2010, p. 56) argued that “ the cyber world provides a convenient platform for criminals to anonymously conduct their illegal activities”.

For cyber criminals the anonymity of the Internet reduces chances of being detected by law enforcement agencies and provides improved safety against other criminals who potentially want to harm them. This high level of anonymity associated with the Internet alongside the use of anonymization procedures makes it difficult for law enforcement to identify cyber criminals and prosecute them (Lusthaus 2012, pp. 71- 72).

Public and private sectors

The current independency of both public and private sectors have put both sectors at a disadvantage when it comes to protecting them against cybercrimes. The European Commission (2012) argue that " no crime is as borderless as cybercrime, requiring law enforcement authorities to adopt a coordinated and collaborative approach across borders, together with public and private stakeholders alike".

A public-private partnership (PPP) would see public and private sectors having secure and trusted information sharing mechanisms. This would allow both sectors to share classified or sensitive information internationally and domestically and have actionable and timely cyber alerts (Choo 2011, pp. 726-727).

Choo (2011, p. 726) states " law enforcement agencies can help in developing and validating effective measures and mitigation controls in collaboration with the private sector by sharing classified or sensitive information such as intelligence and software/hardware vulnerabilities discovered in the course of a law enforcement investigation with the manufacturers and vendors". This allows both sectors to stop cyber attacks

by developing real time mechanisms. A proven example of the success of PPP is in the United States where there is real time operation intelligence provided for critical infrastructure through public and private information sharing and analysis centres (The House Standing Committee on Communications 2010, p. 100).

Central reporting portal

A central reporting portal would allow a range of cybercrimes (malware, spam, scams, fraud etc) to be reported. This would allow for data collection and analysis, which strengthens the detection of organized crime and will support law enforcement efforts across jurisdiction. The House Standing Committee on Communications (2010, pp. 85-86) argue that a central reporting portal “ could greatly enhance law enforcement’s ability to respond to only the immediate crimes and not spend as much time fielding general questions”. Central reporting panels currently exist in the US, Canada and the UK, but should exist in more countries to reduce the harm caused by cybercrimes.

Cooperative and coordinated international response

Cybercrime is an international problem that requires a cooperative and coordinated international response (Broadhurst 2006, p. 412). Esposito (2004) states that “ the fight against cybercrime is either a global one or it makes no sense”. Differences in international laws and the capacity of international law enforcement agencies to enforce these laws can create difficulties cultivating effective international cooperation against cybercrime. Cyber criminals can exploit these inconsistencies as they operate in

countries with weak law enforcement and weak laws. This situation can be improved be encouraging countries to harmonize and strengthen their domestic cybercrime legislation and develop stronger law enforcement capabilities.

Australia is signed and ratified to the Council of Europe Convention on Cybercrime. The Council of Europe (2004) states that “ the Convention aims to develop a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation”. Australia is 1 of 54 countries that have acceded to the Convention. Countries that aren’t acceded include Russia, Mexico, Colombia, and Philippines etc. To further develop international cooperation against cybercrime these countries amongst others must sign and ratify to the Convention. This will ensure that cyber criminals can no longer operate in countries where weak law and enforcement exists.

Conclusion

This essay has examined cybercrime and compared it to traditional crime and found that the challenges imposed by cybercrime include territorial jurisdiction problems, increased global reach for perpetrators and increased anonymity for cyber criminals. To minimalize the harms of cybercrime it is suggested that a public-private partnership is formed, central reporting panels are introduced and international cooperation should be improved through more countries acceding to the Convention.

Reference List:

- Brenner, W & Koops, J 2004, ‘ Approaches to Cybercrime Jurisdiction’, *Journal of High Technology Law,* vol. 4, no. 1, p. 6, viewed 24th April 2017, (online Hein Online)
- Brenner, W & Koops, J 2004, ‘ Approaches to Cybercrime Jurisdiction’, *Journal of High Technology Law,* vol. 4, no. 1, pp. 6-7, viewed 25th April 2017, (online Hein Online)
- Broadhurst, R 2006, ‘ Developments in the global law enforcement of cybercrime’, *Policing: An international Journal of Police Strategies and Management,* vol. 29, no. 3, p. 409, viewed 25th April 2017, (online emerald insight)
- Broadhurst, R 2006, ‘ Developments in the global law enforcement of cybercrime’, *Policing: An international Journal of Police Strategies and Management,* vol. 29, no. 3, p. 412, viewed 25th April 2017, (online emerald insight)
- Broadhurst, R 2006, ‘ Developments in the global law enforcement of cybercrime’, *Policing: An international Journal of Police Strategies and Management,* vol. 29, no. 3, p. 422, viewed 25th April 2017, (online emerald insight)
- Broadhurst et al. 2014, ‘ Organisations and Cybercrime: An analysis of the nature of groups engaged in cybercrime’, *International Journal of Cyber Criminology,* vol. 8, no. 1, p. 13, viewed 25th April 2017,
- Choo, R 2011, ‘ The cyber threat landscape: Challenges and future research directions’, *Computer and security,* vol. 30, pp. 726-727, viewed 23rd April 2017, (online Science Direct)
- Clough, J 2011, ‘ Cybercrime’, *Commonwealth Law Bulletin,* vol. 37, no. 4, p. 673, viewed 22nd April 2017, (online tandfonline)

- Council of Europe 2012, Convention on Cybercrime, viewed 27th April 2017, < https://www. coe. int/en/web/conventions/full-list/-/conventions/treaty/185>
- European Commission 2012, Tackling crime in our Digital Age: Establishing a European Cybercrime Centre, European Union Law, viewed 23rd April 2017, < http://eur-lex. europa. eu/legal-content/EN/TXT/? uri= CELEX%3A52012DC0140>
- Esposito, G 2004. ‘ The Council of Europe Convention on cyber-crime: a revolutionary instrument’, Proceedings of the 2nd Asia Cyber-Crime Summit, viewed 28th of April 2017, (online University of Hong Kong).
- Fossi et al. 2009, ‘ Symantec Report on the Underground Economy’, *The Journal of Financial Services Technology’,* vol. 3, no. 1, p. 77, viewed 20th April 2017, (online FPS Private Wealth)
- Fossi et al. 2009, ‘ Symantec Report on the Underground Economy’, *The Journal of Financial Services Technology’,* vol. 3, no. 1, p. 78, viewed 21st April 2017, (online FPS Private Wealth)
- International Telecommunication Union 2016, Measuring the Information Society Report, p. 209, viewed 22nd April 2017,
- Iqbal et al. 2010, ‘ Mining write prints from anonymous e-mails for forensic investigation’, *Digital Investigation,* vol. 7, p. 56, viewed 23rd April 2017, (online Science Direct)Koops, J 2011, ‘ The Internet and its Opportunities for Cybercrime’, *Tilburg Law School Legal Studies,* vol. 1, no. 09, p. 737, viewed 20th April 2017, < https://papers. ssrn. com/sol3/papers. cfm? abstract_id= 1738223>

- Kshetri, N 2006, ‘ The Simple Economics of Cybercrimes’, *IEEE Computer Society,* vol. 4, no. 01, p. 38, viewed 25th of April 2017, (online IEEE xplore digital library)
- Lusthaus, J 2012, ‘ Trust in the world of cybercrime’, *Global crime,* vol. 13, no. 2, pp. 71-72, viewed 23rd April 2017, (online tandfonline)
- Lusthaus, J 2012, ‘ Trust in the world of cybercrime’, *Global crime,* vol. 13, no. 2, pp. 80, viewed 27th April 2017, (online tandfonline)
- Norton 2016, Norton Cyber Security Insights Report 2016, viewed 21st April 2017, < http://now. symassets. com/content/dam/content/en-au/collaterals/datasheets/norton- cyber-security-insights-report2016. pdf>
- The House Standing Committee on Communications 2010, *‘ Hackers, Fraudsters and Botnets: Tackling the Problem of Cybercrime’* , Nature, Prevalent and Economic Impact of Cybercrime, p. 10, viewed 22nd April 2017,
- The House Standing Committee on Communications 2010, *‘ Hackers, Fraudsters and Botnets: Tackling the Problem of Cybercrime’* , Nature, Prevalent and Economic Impact of Cybercrime, p. 29, viewed 22nd April 2017,
- The House Standing Committee on Communications 2010, *‘ Hackers, Fraudsters and Botnets: Tackling the Problem of Cybercrime’* , Nature, Prevalent and Economic Impact of Cybercrime, pp. 29-31, viewed 22nd April 2017,
- The House Standing Committee on Communications 2010, *‘ Hackers, Fraudsters and Botnets: Tackling the Problem of Cybercrime’* ,

Domestic and International Coordination, pp. 85-86, viewed 22nd April 2017,

- The House Standing Committee on Communications 2010, ‘ *Hackers, Fraudsters and Botnets: Tackling the Problem of Cybercrime’* , Domestic and International Coordination, pp. 93, viewed 22nd April 2017,
- The House Standing Committee on Communications 2010, ‘ *Hackers, Fraudsters and Botnets: Tackling the Problem of Cybercrime’* , Domestic and International Coordination, p. 100, viewed 22nd April 2017,
- Wall, D 2004, ‘ What are Cybercrimes’, *Criminal Justice Matters,* vol. 58, no. 1, pp. 20-21, viewed 21st April 2017, (online tandfonline)