Full paper

Sains Humanika

Understanding Cybercrime in Malaysia: An Overview

Prasad Jayabalan*, Roslina Ibrahim, Azizah Abdul Manaf

Advanced Informatics School, Universiti Teknologi Malaysia (UTM), Jalan Semarak 54100 Kuala Lumpur, Malaysia

*Corresponding author: jprasad@dr.com

Abstract

Rapid developments of internet technology and cyber world have created new opportunities for irresponsible people to take advantage of internet users. Millions of internet users across globe have fallen victim to cybercrime. However, many issues regarding cybercrime are not fully understood yet. It is important to thoroughly understand many aspects of cybercrime for better decision making. This paper provides an overview of cybercrime in Malaysia including current state and statistics of cybercrime, common types of cybercrime, brief description of Malaysian cyber laws and describes the role of Malaysian government in responding to cyber security incidents. Hopefully, this paper will enrich current scenarios of cybercrime in Malaysia. Finally, the directions for future research were discussed.

Keywords: Cybercrime; internet crime; cyber legislation

Abstrak

Perkembangan pesat teknologi internet dan dunia siber telah mencipta pelbagai peluang baru bagi orang-orang yang tidak bertanggungjawab untuk mengambil kesempatan terhadap pengguna internet. Berjuta-juta pengguna internet di seluruh dunia telah menjadi mangsa jenayah siber. Walaupun begitu, masih banyak isu mengenai jenayah siber belum difahami sepenuhnya. Adalah penting untuk benar-benar memahami pelbagai aspek jenayah siber untuk membuat keputusan yang lebih baik. Artikel ini memberikan gambaran keseluruhan jenayah siber di Malaysia termasuk keadaan semasa dan statistik jenayah siber, jenis-jenis jenayah siber, penerangan ringkas undang-undang siber Malaysia dan peranan kerajaan Malaysia dalam menangani isu jenayah siber. Diharapkan artikel ini akan memperkayakan lagi senario semasa jenayah siber di Malaysia. Sebagai pengakhiran, hala tuju kajian seterusnya juga turut dibincangkan.

Kata kunci: Jenayah siber; undang-undang siber

■1.0 INTRODUCTION

Cybercrime is the one of the most feared problem in the internet world. Cybercrime originated prior to the existence of Microsoft Windows, the Internet, or the personal computer (PC) (Thomas, 2006). Year 1964, the first officially recorded incident of cybercrime occurred when a Massachusetts Institute of Technology (MIT) student used an MIT computer to populate the tones necessary to access the long distance phone service (Thomas, 2006). Since then, cybercrime has been a growing national concern due to its destructive financial consequences. Cybercrime is growing quickly compared to other crime types and causing serious destruction to political, economic and social sectors (Hong Lu *et* al., 2010).

The 2012 Norton Cybercrime Report (2012) disclosed that over 556 million people were victims of cybercrime which details down to 1.5 million victims per day and 18 victims per second. With findings based on self-reported experiences of more than 13,000 adults across 24 countries, these criminal acts resulted in $110 billion in direct financial losses which details down to $197 average cost per victim. The Kaspersky Security Bulletin 2013 (2013) disclosed that the average global internet threat level grew by 6.9 percentage points and 41.6% of internet users encountered attack at least once. Malaysia has been ranked 17th with the highest risk of computer infection via internet. Top 20 countries with the highest risk of computer infection via intenet are illustrated in the Table 1. In addition, Bernama reported CyberSecurity Malaysia business development chief Mohd Anwer Mohamed Yusoff as saying that Malaysian has recorded about MYR 2.75 billion in losses in the last five years, mainly due to from cybercrime specific to the financial sector (Cyber Security Malaysia, 2012).

Research in the field of cybercrime requires constant review in providing current status as well as simulating new research initiatives (Wingyanching *et* al., 2004). In this paper, the author provides definitions of cybercrime based on previous researchers, types of cybercrime, legislation and organizational approach to cybercrime in Malaysia.

Table 1 Top 20 countries with the highest risk of computer infection via internet adapted from Kaspersky Security Bulletin 2013 [28].

	Country	**% of unique users**
1	Azerbaijan	56.29%
2	Kazakhstan	55.62%
3	Armenia	54.92%
4	Russia	54.50%
5	Tajikistan	53.54%
6	Vietnam	50.34%
7	Moldova	47.20%
8	Belarus	47.08%
9	Ukraine	45.66%
10	Kyrgyzstan	44.04%
11	Sri Lanka	43.66%
12	Austria	42.05%
13	Germany	41.95%
14	India	41.90%
15	Uzbekistan	41.49%
16	Georgia	40.96%
17	Malaysia	40.22%
18	Algiers	39.98%
19	Greece	39.92%
20	Italy	39.61%

■2.0 DEFINITION OF CYBERCRIME

What is the definition of cybercrime? Cybercrime is not new but there is significant confusion among academics, computer security experts, law enforcement agency and users as to the real definition of cybercrime (Sarah Gordon *et* al., 2006). There are variation of view of what cybercrime is and the lack of clarity in definition is affecting every aspect of prevention and remediation of cybercrime (Sarah Gordon *et* al., 2006). CyberSecurity Malaysia in their official website has stated that “There is no comprehensive definition of cybercrime. There were some attempts but no conclusive definition was agreeable. Cybercrime comes under three categories. The first is when information and communications technology (ICT) systems and intellectual property become targets of exploitation, intrusion, identity and information theft. The second is when ICT devices are used as means to commit crimes. For example, computers at home are used to run malicious programs to intrude other computers to steal money, identity and passwords. The third category is where the ICT devices are used as mediums of committing crimes. For example, sedition, disharmony or unrest, slandering and instigating at higher scale come under this category. Some people say these cases must be prosecuted under cyber laws. But there are already laws that can be used to handle these cases. For example, for sedition and slander, one can be charged under the Penal Code.” (Cyber Security Malaysia, 2013).

Babu and Parishat (2004) described cybercrime as “…a criminal activity committed on the Internet”, while Moitra (2005) described cybercrime occurrences where Internet is involved. Philippsohn (2001) considers cybercrime to exist specifically on the Internet. Many researchers agree that illegal activities performed using computer as the medium and internet or network as the location for the occurrences of cybercrime but the recent research by the 2012 Norton Cybercrime Report (2012) disclosed that cybercrime goes mobile and 2/3 of adults use a mobile device to access the internet. In addition, 31% of mobile users received a text message from someone they didn’t know requesting that they click on an embedded link or dial an unknown number to retrieve a “voicemail”.

Computer Crime Research Center (2011) states that adoption of mobile devices is disclosing opportunities for intrusion and cybercriminals are targeting mobile users, “The emergence of the SymbOS/Zitmo. Altr Trojan in 2009 was evidence of the trend. It was the first appearance of mobile malware in the form of a Trojan horse, a program in which malicious or harmful code is used to steal banking information by keystroke logging”. This paper describes “cybercrime” as illegimate use of ICT devices to conduct criminal activities through electronic networks.

■3.0 AN OVERVIEW OF CYBERCRIME

There are **s**everal issues that teachers have to deal with regarding vocabulary teaching and learning; namely context, number of repetitions, type of words chosen, number of words chosen and level of processing.

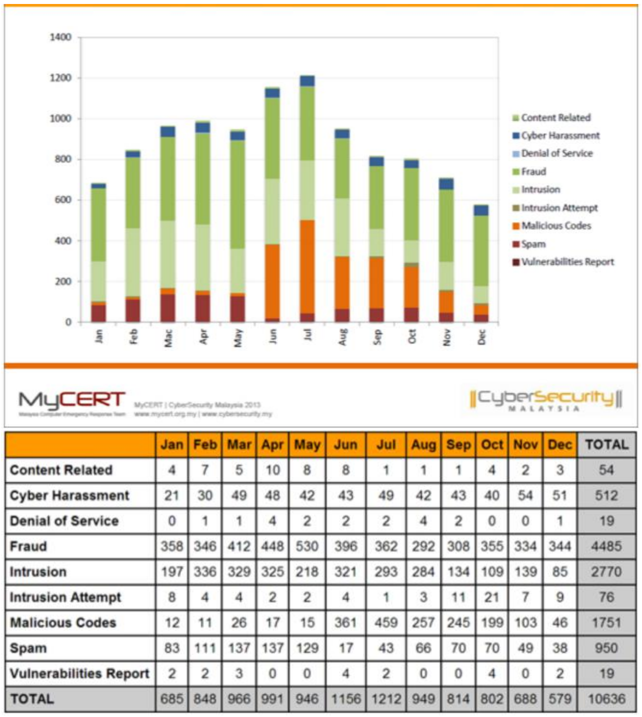
Malaysia is known as one of the Asia's most appealing countries for cyber criminals activities. According to the Internet World Stats (2012) Malaysia’s total number of Internet users reached an estimated 17 million by June 2012 whereas the percentage of Malaysia Internet users growth is 356.8 percent from 2000 to 2010. China’s total number of Internet users reached an estimated 538 million by June 2012, making it the largest Internet user nation. The wide usage of internet is opening opportunities making it vulnerable to cybercriminals. The nature of internet itself has provided a platform for cybercriminal to conduct illegal activities from anywhere in the world. According to the 2010 Norton Cybercrime Report (2010), up to 83 percent of Internet users in Malaysia have fallen victim to cybercrimes. 45 percent of cybercrime victims in Malaysia have never fully resolved the cybercrime and it takes an average of 30 days and an average cost of MYR7,323 to come to a resolution. 20 percent of the respondents said the biggest problem they faced when associated with cybercrime was the loss of irreplaceable data; and 60 percent said their biggest fear is the financial loss.

Malaysia's Internet infrastructure was attacked by the Code Red worm in 2001 which interrupted our national communication network and caused estimated minimum losses of RM22mil. The affected agencies took total duration of 3 months to eliminate the worm. In 2003, our nation was again under attack by the Blaster and Naachi worms which caused estimated cost of RM31mil to eliminate these worms. These worms have focused on the vulnerability in the operating systems of Windows NT, 2000 and XP through scanning the computers via network (Zahri Yunos, 2008). Both incidents caused business disruption and reputation damage.

According to Deputy Inspector-General of Police Malaysia, Datuk Seri Mohd Bakri Mohd Zinin (Dhashene Letchumanan, 2013) based on the Sophos Security Threat Report 2013 by the firm SOPHOS USA, in the first three months of 2013, Malaysia was ranked sixth in the world of high-risk exposure to cybercrime threat. In addition, Bakri shared that losses amounted to RM1.115 billion with 8,920 of the 11,543 reported cases solved and 3,712 people arrested last year.

3.1 Types of Cybercrime

What are the different types of cybercrime? According to a report by Malaysia Computer Emergency Response Team (MyCERT), that deals with all security incidents reported by commercial victims. MyCERT has classified cybercrime into 9 categories. Security incidents statistics for the year 2013 are illustrated in the Figure 1 (Malaysia Computer Emergency Response Team, 2013a).



	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	TOTAL
Content Related	4	7	5	10	8	8	1	1	1	4	2	3	54
Cyber Harassment	21	30	49	48	42	43	49	42	43	40	54	51	512
Denial of Service	0	1	1	4	2	2	2	4	2	0	0	1	19
Fraud	358	346	412	448	530	396	362	292	308	355	334	344	4485
Intrusion	197	336	329	325	218	321	293	284	134	109	139	85	2770
Intrusion Attempt	8	4	4	2	2	4	1	3	11	21	7	9	76
Malicious Codes	12	11	26	17	15	361	459	257	245	199	103	46	1751
Spam	83	111	137	137	129	17	43	66	70	70	49	38	950
Vulnerabilities Report	2	2	3	0	0	4	2	0	0	4	0	2	19
TOTAL	685	848	966	991	946	1156	1212	949	814	802	688	579	10636

Figure 1 Security Incidents Statistics for year 2013 adapted from Malaysia Computer Emergency Response Team (MyCERT)

The description of each cybercrime category as follows (Malaysia Computer Emergency Response Team, 2013b):

3.1.1 Content Related

Content related refers to material which is offensive, morally inappropriate and does not adhere to current standards of accepted behavior (Malaysia Computer Emergency Response Team, 2013b). Content related is further broken into pornography, national threat and intellectual properties. Pornography refers to excessive content by accepted standards of morality and decency. National threat refers to content that reasons displeasure, communicates intent to incite harm or loss, an indication of impending danger to public is deliberated and is illegal.

Intellectual properties refers to cases where there is unauthorized use of any word, name, symbol, or device used by individual or organization to identify and distinguish his or her goods, including a unique product, from those manufactured or sold by others and to indicate the source of the goods. There are a total of 20 cases reported in the year of 2012 for content related cybercrime (Malaysia Computer Emergency Response Team, 2012).

3.1.2 Cyber Harassment

Cyber harassment is generally understood as conduct intended to annoy, distract or intrude. In terms of legal, it is a conduct which refers to intimidating or disrupting. Cyber harassment is further broken into cyber bullying, cyber stalking, racial, religious and sexual (Malaysia

Computer Emergency Response Team, 2012). Cyber bullying refers to any information and communication technology devices that are used to communicate pictures or even test messages with a reason to harass or humiliating another individual. Cyber stalking refers to any electronic communication method for instance electronic email or messaging or uploading to a website, groups chat. A cyber stalker generally takes advantage of the anonymity on the internet to intimidate victim without being traced. Please note that this is not spamming. Cyber stalker targets definite victim with intimidating messages whereas spammer targets multiple victims with disturbing messages. Racial and religious harassment refers to abusive, insulting, obnoxious or unapproachable remarks towards victims. Remarks towards victim contains unfavorable, expletive, disapproving and often damaging with regards to the subject's racial and religion religion. Sexual harassment refers to any information and communication technology devices used to send photos or text messages with the objective of humiliating or offending another individual. Sexual harassment contains unpleasant remarks about person's physical appearance sexually. There are a total of 300 cases reports in the year of 2012 for cyber harassment (Malaysia Computer Emergency Response Team, 2013b).

3.1.3 Denial of Service

A denial of service (DOS) attack is an attempt by a website being flooded with data with the objective of making it unavailable for authorized users accessing it. Organizations are subject to suffer high financial losses as it can take couple of hours to recover (BBC News, 2001). There are a total of 23 cases reports in the year of 2012 denial of service (DOS) attack (Malaysia Computer Emergency Response Team, 2013b).

3.1.4 Fraud

The term fraud generally refers to any type of fraud scheme that uses one or more online services to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme. Fraud is further broken into phishing, fraud site, fraud purchase, counterfeit item, online scam, unauthorized transaction, illegal investment, lottery scam and Nigerian scam. Phishing refers to criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or online banking are commonly used to lure the unsuspecting public. Phishing is typically carried out by e-mail or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Fraud site refers to website created by scammer to entice user on acquire their service or buy certain product which actually not providing actual goods or services. This particular fraud site also has the possibility embedded with Malware / Trojan software in which will infected unsuspected visitors. Fraud purchase refers to purchasing good or services by using bogus credit card or stolen online/internet banking credential. Counterfeit item refers to selling or limiting goods or money intended to deceive or defraud online user. Counterfeited goods of inferior quality are often sold at substantially lower prices than genuine products and may bear the brand or trade name of the company. Counterfeiting violates trademark and intellectual property rights and may damage the reputation of producers of authentic goods. Online scams refers to using online services to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme. Unauthorized transaction refers to trying to gain access into any computer, network, storage medium, system, program, file, user area, or other private repository, without the express permission of the owner. Unauthorized access is the same as theft. Example Use of a Credit Card by someone other than the authorized cardholder, for example, after a bank credit card has been lost or stolen and purchases not approved by the cardholder are charged to the account. Illegal investment refers to a fraudulent moneymaking scheme in which people are recruited to make payments to others above them in a hierarchy while expecting to receive payments from people recruited below them. Eventually the number of new recruits fails to sustain the payment structure, and the scheme collapses with most people losing the money they paid in. Lottery scam refers to a common internet scam where there is no lottery and no prize. Those who initiate a dialogue with the scammers by replying to the lottery scam emails will eventually be asked for advanced fees to cover expenses associated with delivery of the supposed "winnings". Nigerian scam refers to one of the most common types of fraudulent email currently hitting inboxes. Nigerian scam messages can also arrive via fax or letter. The messages generally claim that your help is needed to access a large sum of money, usually many millions of dollars. In fact, this money does not exist. The messages are an opening gambit designed to draw potential victims deeper into the scam. Those who initiate a dialogue with the scammers by replying to a Nigerian scam message will eventually be asked for advance fees supposedly required to allow the deal to proceed (Malaysia Computer Emergency Response Team, 2013b).

3.1.5 Intrusion Attempt

Intrusion is referred to the unauthorized access or illegal access to a system or network, successfully. This could be the act of root compromise, web defacements, installation of malicious programs, i.e. backdoor or Trojan. Intrusion attempt is further broken down to port scanning, login brute force and vulnerabilities probes. Port scanning refers to the act of systematically scanning a computer's ports. Since a port is a place where information goes into and out of a computer, port scanning identifies open doors to a computer. Port scanning has legitimate uses in managing networks, but port scanning also can be malicious in nature if someone is looking for a weakened access point to break into your computer. Login brute force refers to an exhaustive testing of all possible methods that can be used to break a security system. Vulnerabilities probes refers to an automated process of proactively identifying vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited or threatened (Malaysia Computer Emergency Response Team, 2013b).

3.1.6 Malicious Codes

Malicious code is the term used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system. Malicious code describes a broad category of system security terms that includes attack scripts, viruses, worms, Trojan horses, backdoors, and malicious active content. Malicious code is broken into botnet C&C, bots, malware and malware hosting. Bootnet refers to a jargon term for a collection of software agents, or robots, that run autonomously and automatically. The term is most commonly associated with malicious software, but it can also refer to the network of computers using distributed computing software. While botnets are often named after their malicious software name, there are typically multiple botnets in operation using the same malicious software families, but operated by different criminal entities. Bots can automatically scan their environment and propagate themselves using vulnerabilities and weak passwords. Generally, the more vulnerability a bot can scan and propagate through, the more valuable it becomes to a botnet controller community. The process of stealing computing resources as a result of a system being joined to a "botnet" is sometimes referred to as "scrumping. Malware refers to short for malicious software, is software designed to infiltrate a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code. The term "computer virus" is sometimes used as a catch-all phrase to include all types of malware, including true viruses. Malware hosting refers to where malware reside whether at a comprise server or client personal computer that have been infected by malware (Malaysia Computer Emergency Response Team, 2013b).

3.1.7 Spam

Spam is broken into spam and spam relay. Spam refers to unsolicited e-mail, often of a commercial nature, sent indiscriminately to multiple mailing lists, individuals, or newsgroups; junk e-mail. Spam relay refers to sending mail to a destination via a third-party mail server or proxy server in order to hide the address of the source of the mail. When e-mail servers (SMTP servers) are used, it is known as an "open relay" or "SMTP relay," and this method was commonly used by spammers in the past when SMTP servers were not locked down. Spam frequently is known to be the first touch point for offenders to engage with their victims apart from being constitutes as an illegal criminal act in jurisdiction. Victims tend not to take spam seriously and potentially spam can lead to more significant form of cybercrime occurrences. For example, ‘back doors’ created by Trojans is later used to commit cybercrime in a large scale (BBC News Online, 2013).

3.1.8 Vulnerabilities Report

Security vulnerability is a flaw in a product that makes it infeasible even when using the product properly in order to prevent an attacker from usurping privileges on the user's system, regulating its operation, compromising data on it, or assuming ungranted trust. Vulnerabilities report is broken into misconfiguration, web and system. Misconfiguration refers to a problem exists with certain configuration which may allow root access or system compromise from any account on the system. Web refers to user or complainant report vulnerabilities which related to Web sites. System refers to user or complainant report vulnerabilities on any specific system (Malaysia Computer Emergency Response Team, 2013b).

3.2 Legislation

In response to any type of crime, it has been a practice by our society to prevent the crime and ensure the perpetrators are punished in the first instance itself. How is this being achieved? Creating legislations which clearly states specific activities are illegal is the answer. This is crucial in establishing Malaysia as the leader in ICT and towards achieving vision 2020. The objective of Vision 2020 is Malaysia’s emergence as an economically-developed, industrialized nation by the year 2020. Therefore, Malaysian Government has already passed several cyber laws to control, reduce of cybercrime activities and increase the success rate of prosecuting cybercriminals. The Malaysian Cyber Laws also provides confidents to potential investors that the government has taken seriously the protection of technology itself. The Malaysian cyber law consists of Communication and Multimedia Act 1998, Computer Crimes Act 1997, Digital Signatures Act 1997, Telemedicine Act 1997, Electronic Government’s Activities Act 2007 and Copyright Act (Amendment) 1997. There are other existing laws that may be used to regulate whenever applicable. They are Sedition Act 1948, Penal Code and Defamation Act 1957. This paper will provide a brief description of cyber laws (Ministry of Sceince, Technology & Innovation (MOSTI), 2013).

3.2.1 Communication and Multimedia Act 1998

The Communication and Multimedia Act 1998 (2006) has been enforced by the Malaysian government on 1st April 1999. This act provides defines roles and responsibility of those providing communication and multimedia services. It also creates a new system of licenses. It also stated that there will be no filtering in accessing the Internet in Malaysia. The Act introduces Communication and Multimedia Commission as a new regulatory authority to oversee ICT industry.

3.2.2 Computer Crimes Act 1997

The Computer Crimes Act 1997 (2006) has been enforced by Malaysian government on 1st April 1999. The main reason for enforcing this act is to prevent accessing computer or computer system without authorization. It also ensures that passwords are not given to those who are not legitimate to receive it.

3.2.3 Digital Signatures Act 1997

The Digital Signatures Act 1997 (2006) has been enforced by Malaysian Government on 1st October 1998. The main purpose of this act is to provide both licensing and regulation of Certification Authorities (CA). The Act also makes digital signatures as legally valid and enforceable as a traditional signature. This helps to prevent on-line transaction fraud.

3.2.4 Telemedicine Act 1997

The Telemedicine Act 1997 (2006) has not been enforced as there is amendment still being implied. The act states that only registered doctor will be allowed to practice "telemedicine". Other healthcare providers must first obtain license to practice "telemedicine". This is prohibiting misuse of medical related items.

3.2.5 Electronic Government Activities Act 2007

The Electronic Government's Activities Act 2007 (2007) has been enforced by Malaysian government on 1st January 2008 (Multimedia Development Corporation, 1996-2012). The act is to facilitate electronic delivery on government services to the public.

3.2.6 Copyright Act (Amendment) 1997

The Copyright Act (Amendment) 1997 (1997) has been endorsed on 1st April 1999 by Malaysian government. This act is amendment from Copyright Act 1987. It protects the copyright works from unauthorized copying or alteration.

3.3 Organizational

The Malaysian government has been playing an active role in preventing cybercrime effectively and efficiently. Having said that, the Malaysian government has set up the Cyber Security Malaysia, the national cyber security specialist agency under the Ministry of Science, technology and Innovation (MOSTI). Previously known as the National ICT Security and Emergency response Centre (NISER).As for responding to computer security incidents, Cyber Security created The Malaysian Computer Emergency Response Team (MyCERT) as part of their service offerings. MyCERT consists of specialist in the area of Intrusion Analysts, Malware Analysts, Application Security Analysts, and Emergency Response Professionals. MyCERT operates the Cyber999 Help Centre, a public service that provides emergency response to computer security related emergencies as well as handling incidents such as content related, cyber harassment, denial of service, fraud, intrusion, intrusion attempt, malicious codes, spam, vulnerabilities report and other security incidents.

In the effort to instill awareness among Malaysian, public and private sector are beginning to establish strategic alliances. Limkokwing University of Creative Technology and the Royal Malaysian Police (PDRM) have signed a Memorandum of Understand (MoU). Limkokwing University will assist the Commercial Crimes Investigation Department (CCID) PDRM in providing materials such as posters and video clips. In addition, Limkokwing University also provides advise on the implementation of cybercrime prevention campaign strategy for the next five years (Dhashene Letchumanan, 2013). DIGI Telecommunications Sdn Bhd launched a DIGI CyberSAFE Programme in partnership with Education Ministry, CyberSecurity Malaysia, Childline Malaysia, Malaysian Communications and Multimedia Commissions. The aim of this programme is to raise awareness on online child safety and equipping students, parents and educators with the right tools to enjoy an internet experience without feeling insecure (Zorachan, 2013).

■4.0 FUTURE WORK

This study will further research on the definition of cybercrime as cybercrime goes mobile and propose a more concise definition. Clarity in cybercrime definition will assist law enforcement agencies in responding to cybercriminal activities more effectively and efficiently.

Furthermore, this study will further explore in details on current status of cybercrime in different countries and provide a comparative analysis. With that, the authors hope to provide recommendations for future directions in combating cybercrime.

■5.0 CONCLUSION

In conclusion, cybercrime is growing more quickly than any other crime and affects our nation destructively. In this paper, we have examined some of existing definition of cyber crime and found to be lacking of clarity in the definition of cybercrime. Apart from that, this paper also provides current state and statistics of cybercrime in Malaysia and further describes the common types of cybercrime such as content related, cyber harassment, denial of service, fraud, intrusion, intrusion attempt, malicious codes, spam, and vulnerabilities report.

As for the legislation, Malaysian Government has set up cyber laws to control, reduce of cybercrime activities and increase the success rate of prosecuting cybercriminals. This paper also provides brief description of Communication and Multimedia Act 1998, Computer Crimes Act 1997, Digital Signatures Act 1997, Telemedicine Act 1997, Electronic Government's Activities Act 2007 and Copyright Act (Amendment) 1997. As for the organizational approach against cybercrime, this paper describes the role of Malaysian government in responding to cyber security incidents through Cyber Security Malaysia as well as the strategic alliances between public and private sector in combating cybercrime.

Finally, cybercrime is rapidly evolving and is a crime waiting to happen anytime to millions of Malaysians' internet users. In-depth understanding of many aspects in cyber crime is crucial in order to facilitate the government, enforcement officers as well as increasing public awareness on such crime. This hopefully, will minimize the cyber crime cases and also increasing public resistance from being scammed into such crime.

References

Babu, M., & Parishat, M. (2004). What is cybercrime? Retrieved August 27, 2013, from http://www.crime-research.org/analytics/702/.

BBC News. (2001). Life of Crime Part 5, United Kingdom. Retrieved September 30, 2013 from http://news.bbc.co.uk/hi/english/static/in_depth/uk/2001/life_of_crime/cybercriminals.stm>.

BBC, Spammers and Virus Writers Unite, BBC News Online. (2003). Retrieved June 10, 2014 from http://news.bbc.co.uk/1/hi/technology/2988209.stm.

Communications and Mutimedia Act 1998 (REPRINT). (2006). Retrieved September 30, 2013 from http://www.agc.gov.my/Akta/Vol.%2012/Act%20588.pdf.

Computer Crime Act 1997 (REPRINT). (2006). Retrieved September 30, 2013 from http://www.agc.gov.my/Akta/Vol.%2012/Act%20563.pdf.

Computer Crime Research Center. (2013). Cybercrime Goes Mobile. Retrieved September 29, 2013 from http://www.crime-research.org/news/16.03.2011/3865/.

Cyber Security Malaysia. (2012). Hacking Costs Malaysia MYR 3.3 mln, Telecompapaer (19 nov 2012). Retrieved September 29, 2013, from http://www.cybersecurity.my/en/knowledge_bank/news/2012/main/detail/2249/index.html.

CyberSecurity Malaysia. (2013). What About Cybercrime. Retrieved September 2013, from http://www.cybersecurity.my/en/media_centre/media_faqs/media_faqs/main/detail/1691/index.html.

Copyright Act (Amendment). (1997). Retrieved September 30, 2013 from http://www.myipo.gov.my/documents/10180/23047/Copyright%20(Amendmend)Act%20A994.pdf.

Dhashene Letchumanan. (2013). Lim Kok Wing University and Royal Malaysian Police Fights Cybercrime, Lim Kok Wing University of Creative Technology official website, August 29, 2013. Retrieved September 30, 2013 from http://www.limkokwing.net/media/news/limkokwing_university_royal_malaysian_police_fights_cyber_crime/.

Digital Signatures Act 1997 (REPRINT)**.** (2006). Retrieved September 30, 2013 from http://www.agc.gov.my/Akta/Vol.%2012/Act%20562.pdf.

D. Thomas, B. D. Loader. (2000). Introduction—cybercrime: Law Enforcement, Security and Surveillance in the Information Age, Cybercrime: Law Enforcement, Security and Surveillancein the Information Age, Taylor & Francis Group, New York, NY.

Electronic Government's Activities Act. (2007). Retrieved September 30, 2013 from http://www.mampu.gov.my/documents/10228/11836/Electronic+Government+Activities+Act+2007-Act+680.pdf/e4b7ba49-eec5-42c7-b0f5-a73f6e984767.

Hong Lu, Bin Liang, Melanie Taylor. (2010). A Comparative Analysis of Cybercrimes and Government Law Enforcement in China and United States. Published in Springer Science.

Internet World Stats. (2012). Retreived August 28, 2013 from http://www.internetworldstats.com/stats3.htm.

Kaspersky Security Bulletin. (2013). Statistics, Retrieved June 10, 2014 from http://report.kaspersky.com/#the-overall-statistics-for-2013.

Malaysia Computer Emergency Response Team. (2012). MyCERT Incident Statistics 2012, Retrieved September 29, 2013 from http://www.mycert.org.my/en/services/statistic/mycert/2012/main/detail/836/index.html.

Malaysia Computer Emergency Response Team. (2013a). Definitions of Incidents, 2013a Retrieved June 10, 2014 from http://www.mycert.org.my/en/services/statistic/mycert/2013/main/detail/914/index.html.

Malaysia Computer Emergency Response Team. (2013b). Definitions of Incidents, Retrieved September 29, 2013b from http://www.mycert.org.my/en/services/report_incidents/cyber999/main/detail/799/index.html.

Ministry of Science, Technology & Innovation (MOSTI), Malaysia. (2013). Cyberlaws in Malaysia. Retrieved September 30, 2013, from http://nitc.mosti.gov.my/nitc_beta/index.php/national-ict-policies/cyberlaws-in-malaysia.

Moitra, S. (2005). Developing Policies for Cyber crime. *European Journal of Crime, Criminal Law and Criminal Justice*. 13(3), 435–464.

Sarah Gordon, Richard Ford. (2006). On the Definition and Classification of Cybercrime. Springer-Verlag France.

S. Philippsohn. (2001). Trends in Cybercrime—An Overview of Currentfinancial Crimes on the Internet. *Computers & Security*. 20(1), 53–69.

Telemedicine Act 1997 (REPRINT). (2006). Retrieved September 30, 2013 from http://www.agc.gov.my/Akta/Vol.%2012/Act%20564.pdf.

The Reality of Cyber-Threats Today, Zahri Yunos. (2014). Cybersecurity Malaysia, September 23, 2008, Retrieved June 10, 2014 from www.cybersecurity.my/data/content_files/13/420.pdf.

Thomas, J. (2008). Cybercrime: A Revolution in Terrorism and Criminal Behavior Creates Change in the Criminal Justice System. Retrieved September 30, 2008, from http://www.associatedcontent.com/article/44605/cybercrime_a_revolution_in_terrorism_html?page=2&cat=37.

Wingyanching, Hsinchun Chen, Weiping Chang, Shihchieh Chou. (2004). Fighting Cybercrime: A Review and the Taiwan Experience. Published in Science Direct, September.

Zorachan. (2013). Protection Against Cyber Crime, July 7, 2013, The Star Online. Retrieved September 30, 2013 from http://www.thestar.com.my/story.aspx?file=%2f2012%2f7%2f7%2fsarawak%2f11617870.

(2010). Norton Cyber Crime Report, Retrieved February 23, 2011, from http://www.symantec.com/en/my/norton/theme.jsp?themeid=cybercrime_report.

(2012). Norton Cyber Crime Report, Retrieved September 28, 2013, from http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf.