Analysis of Computer Crime in Singapore using Local English Newspapers

Na Jin-Cheon
Wu Hao, Ji Yong, Tay Mia Hao
Ramanathan Mani Kandan
Nanyang Technological University

Abstract

The purpose of this study was to collect and analyze computer crime cases in Singapore over a 6-year period from 2003 to 2008, and to understand the trend in computer crimes. For data collection, we constructed comprehensive query terms for searching all the computer crime cases in Singapore. All the related terms for "computer crime" were collected using two thesauri engines which were namely Inspect and Compendex. In the search phase, the two search engines, LexisNexis Academic and Factiva, were employed. The source of the articles was all English newspapers published in Singapore, such as The Straits Times, The Business Times, and Today. Based on the collected computer crime cases in Singapore, the top three computer crimes categories were hacking (32.4%), fraud (29.5%), and intellectual property theft (17.1%). Among these three categories, fraud had increased from 12.5% to 42.9% of total cases in the 6-year period. The analysis showed that the offenders were mainly male (90.3%) and in the age group between 18 and 40 years old (75%); 73.9% of the criminals had university or polytechnic education; 46.6% were at either management/professional or executive positions.

Keywords: Computer crime, Singapore

Introduction

The security of computer systems was threatened by intentional and unintentional acts, both internally and externally. Newman (2006) indicated that computer attacks were classified as either active or passive. An active attack involves some modification of the data stream or attempts to gain unauthorized access to computer and networking systems. A passive attack would include monitoring and eavesdropping on a transmission. Generally there were various methods of attack used in computer crime such as brute force attack, masquerading, address spoofing, session hijacking, replay attack, man-in-the-middle attack, dictionary attack, boot sector viruses, and war dialers. Byers, Rubin, and Kormann (2004) studied Internet-based attacks on the physical world. As more business operation functionalities have moved online, and as more services were automated, there was a greater risk that cyber attacks can cause problems that were manifested in the physical world.

Computer crime specifically means criminal activities against a computer or facilitated by or committed by the use of a computer. Generally the definition of computer crime was often complicated by the fact that an act may be illegal in one nation but not in another. The United States Department of Justice categorizes computer crime in three ways: using the computer as a target – attacking the computers of others (e.g. spreading a virus); using the computer as a tool – using a computer to commit "traditional crime" (e.g. illegal gambling); using the computer as an accessory – using a computer to store illegal or stolen information (Cybercitizenship.org, 2009).

The following lists some typical computer crime types due to the increasing dependence of business on computer systems (Business Software Alliance, 2009):

- Financial: crimes that disrupt a company's e-business or steal confidential files for ransom
- Piracy: crimes of copying and distributing copyrighted works without permission
- Hacking: crimes of gaining unauthorized access to a computer system or network
- Pornography: crimes of distributing pornography in any form to a minor

- Cyber-terrorism: distinguished by its purpose and severity, which was designed to cause violence against persons or property, or at least cause enough harm to generate fear

As computer crime was often seen and reported in the Western world, most studies in the literature focused on big countries like the US and UK (Richardson, 2007; Hinduja, 2007; Barton & Nwassanka, 2003; Bigelow, 1993; Nigri, 1992) and very few for a small country like Singapore. Singapore was one of the countries with the lowest crime rates in the world. At the same time, it was also identified as the most network ready country (John, 2006). In Singapore, about 75 percent of all households were connected to the Internet, 10 percent of Web surfers use their connection primarily for social networking, and 12 percent use it for interactive online games (Luo, 2008). There has been a proliferation of computer crime in Singapore despite its low crime rate.

The purpose of this study was to examine the computer crime cases in Singapore, identify their patterns and methods, and show the trend and demographic characteristics of criminals. This study investigated six years of computer crime cases, from 2003 to 2008. The data sources were from Singapore English language newspapers (e.g. The Straits Times, The Business Times, and Today) available in the two databases, LexisNexis Academic and Factiva. After gathering all the computer crime cases, data and trend analyses were performed on the raw data. The different categories for the computer crime cases included fraud, spamming, hacking, intellectual property theft, identity theft, and harassment. Apart from delving into the trends in Singapore computer crime, we also analyzed computer crime cases which had taken place in Hong Kong, Malaysia, Thailand, and India, and compared these cases with those in Singapore.

Literature Review

Relevant work has been done mostly in developed countries, but not many studies have been done in Singapore regarding computer crime. Most of literature studied the impact of computer crime, conducted surveys and trend analysis of the public and corporate sectors. The recent studies conducted in

various countries showed that computer crime was increasing in an alarming rate and becoming a serious threat.

Computer Crime Studies

In the US, a computer crime and security survey was conducted by Computer Security Institute (CSI) (Richardson, 2007). Based on the responses of 494 computer security practitioners in American corporations, government agencies, financial institutions, medical institutions, and universities, the top 10 types of attacks or misuse with the percentage given in parentheses:

- Insider abuse of net access (59%)
- Virus (52%)
- Laptop/mobile device theft (50%)
- Phishing (26%)
- Instant messaging misuse (25%)
- Denial of service (25%)
- Unauthorized access to information (25%)
- Bots within the organization (21%)
- Theft of customer/employee data (17%)
- Abuse of wireless network (17%)

The survey also showed that the total losses for 2007 added up to US$66,930,950 based on 194 responses, up from US$52,494,290 (for 313 respondents) in 2006. The average loss per respondent was $345,005 for 2007, up from $167,713 in 2006. In terms of amount of losses by type of attack, financial fraud registered the highest amount (US$21,124,750) followed by virus (worms/spy ware) (US$8,391,800).

In Taiwan, as another example, Chen et al. (2005) analyzed cybercrime activity and reported that the number of thefts, fraudulent activities, robberies, counterfeited documents, assault and batteries, threats, and illegal gambling cases from online games increased to 1,300 cases from 55 only two years earlier; furthermore, online gaming-related crime became the most serious problem within all cyber-criminal cases. The research findings from Chung et al. (2006) showed that cybercrime was mainly conducted by highly-educated

people, and sex trading on the Internet (34%) and stealing treasure (money credits) for cyber-games (20%) accounted for most cybercrime between 1999 and 2002 in Taiwan.

In Singapore, the rising computer crime cases have received the Singapore government's attention. Chua (2005) reported that a total of $38 million Singapore dollars had been set aside by the government to beef up Singapore's cyber-security defenses over the next three years. Dr Tony Tan Keng Yam, the former Deputy Prime Minister in Singapore, announced this at the unveiling of the Infocomm Security Masterplan, which aimed to help Singapore expand its capabilities in cyberspace security. Noting how infocomm technology has become the "nerve centre of Singapore's economy" and "an intricate component of infrastructure in critical sectors", Dr Tan emphasized that "because Singapore was so networked, a comprehensive security plan for Singapore's infocomm security was vital to prevent our economy and society from being disrupted in the event of an attack."

A fraud survey report by audit firm, KPMG Singapore, identified a big rise in computer-related fraud in Singapore (KPMG, 2008). For the 2004 survey, just 19% of the firms polled reported fraud incidents, and the figure had risen to 59% in 2007. The report said the computer-related fraud had emerged as "the fastest-growing and most pervasive category of fraud" in Singapore. Gwee (2008) reported that "Singapore has the second highest number of cyber-bullying cases after the US" based on studies published by WiredSafety.org. In 2006, 25% of 3,488 Singaporean students polled reported having been victimized online.

Sophos, an IT security and control firm, published a report which studied the security threat situation in 2008 (Choudhury, 2009). The Sophos report revealed that in 2008, 37% of all global malware was hosted in the US. China was second with 27.7%, then Russia with 9.1%. In comparison, Singapore was responsible for less than 0.1% of global malware hosting. For spam, in 2008, the US was top with 17.5%, down from 22.5% in 2007, and followed by Russia with 7.8%. Turkey was an unexpected third with 6.9% and China fourth with 6%. In comparison, spam produced in Singapore was 0.3%, giving the island a global ranking of 39 out of 240 countries.

Cyberspace Rules and Regulations in Singapore

There were various regulations and acts specific for the online environment in Singapore. Singapore cyberspace rules and regulations generally follow the international cyberspace rules. As an initial effort for securing computer materials against unauthorized access or modification, the Computer Misuse Act was introduced as Act 19 in 1993, and current version was the 2007 revised edition (Attorney-General's Chambers, 2009). The revised Act takes a more sophisticated approach to provide penalties proportionate to the different levels of potential and actual harm caused. It also addresses new potential computer abuses such as unauthorized use or interception of computer service, unauthorized obstruction of use of computer, and unauthorized disclosure of access code.

Endeshaw (1999) investigated computer misuse law in Singapore. The paper covered the Computer Misuse Act 1993, criminal laws, and conflicts between them. Carr and Williams (2000) compared the three laws, UK Computer Misuse Act 1990 (UKCMA), Malaysian Computer Crimes Act 1997 (MCCA), and Singapore Computer Misuse Act (SCMA) 1993, in view of the powers of investigation and the penalty levels, as well as the amount of use to which these laws were put once enacted. Cerezo et al. (2007) reported that the main challenges faced by law endowment were the lack of harmonization of national criminal laws and the difficulties of finding a definition of computer related crime.

The Spam Control Act was passed by Singapore Parliament as Act 21 in 2007, and current version was 2008 revised edition (Attorney-General's Chambers, 2009). This Act provides for the control of spam, which was unsolicited commercial communications sent in bulk by electronic mail or by text or multi-media messaging to mobile telephone numbers. This was a relatively new Act in reflection of the evolution of the Internet and cyberspace in which the recent years has seen an increase of a new way of advertising, i.e. spam. Business and the industry that operates with/in the Internet were also obligated to follow regulations, such as the Electronic Transaction Act. The Electronic Transaction Act was first in effect as Act 25 in 1998, and the current version was the 1999 revised edition, which was amended in 2004 (Attorney-General's Chambers, 2009). The Electronic Transaction Act governs the security and use of electronic transactions.

Research Methodology

For data collection, we constructed comprehensive query terms for searching all the computer crime cases in Singapore. All the related terms for "computer crime" were collected using two thesauri engines namely Inspec and Compendex. The related query terms were shown in Table 1. For instance, "computer viruses" and "computer worms" were added to the query terms as *Narrower Terms*, and "unsolicited e-mail" and "spamming" as *Related Terms*.

Table 1: Related terms for "computer crime"

	Thesauri Engines	
Term Types	**Inspec**	**Compendex**
Exact Term	computer crime	computer crime
Used for	hacking (illegal computer access) piracy, software software piracy	crime (computer) hacking (computer crime) software piracy
Prior Terms	security of data	
Top Terms	security	
Broader Terms	security of data	computer applications
Narrower Terms		*computer viruses* *computer worms*
Related Terms	computer viruses, criminal law, data privacy, fraud, government policies, invasive software, legislation, and *unsolicited e-mail*	computer privacy, computer system firewalls, computers, data privacy, law enforcement, security of data, security systems, and *spamming*

In the search phase, the two search engines, LexisNexis Academic and Factiva, were employed. The sources of the articles were the English language newspapers published in Singapore. With the returned articles from the search engines, the following factors were taken into consideration for identifying whether the articles were computer crime cases in Singapore:

- Did the reported case happen in Singapore and not another country?
- Was the reported case discovered by the police in the time period specified from 2003 to 2008?
- Did the reported case have the computer crime indicator, i.e. court sentence, jail/fine, Computer Misuse Act, punish, guilty, charge, arrest, and raid.

Table 2 shows the statistics for the collected computer crime cases. Duplicated computer crime cases were filtered by reading the relevant articles again. Only 105 cases were collected from the newspapers. We believed that there could be additional computer crime cases not reported in the newspapers. Cerezo et al. (2007) argued that there were many unreported or unknown computer crime cases due to high-level technology, lack of training of investigating officials, unknown victims, disinclination of victims to report them, difficulties in locating and identifying perpetrators across borders, and other computer procedural problems. Sukhai (2004) also mentioned that companies were afraid that the competitors would capitalize on the bad publicity if they reported the incident to the authorities and that only 15% of such attacks were reported to the law enforcement agencies.

Table 2: Statistics for Computer Crime Cases from 2003 to 2008

Year	No. of Articles Found	Relevant Articles	Repeated Cases	No. of Computer Crime Cases (duplicates removed)
2003	8169	9	1	8
2004	9348	13	3	10
2005	10461	19	1	18
2006	11826	33	11	22
2007	10977	37	11	26
2008	12507	29	8	21
			Total Cases:	105

Analysis of Computer Crime Cases in Singapore

From the collected computer crime cases, we identified six computer crime categories or types. Each computer crime case was assigned one of the six categories. Table 3 shows the brief definition and some examples of the six categories.

Table 3: Categories of Computer Crimes

Category	Description
Fraud	Fraud achieved by the manipulation of computer records or phishing e-mail Salami slicing which was the practice of stealing money repeatedly in extremely small quantities Industrial espionage by means of access to or theft of computer materials
Spamming	Spamming which involves sending unsolicited emails and SMS (Short Message Service) to public without consent
Hacking	Unauthorized access to or modification of program or data Deliberate circumvention of computer security systems Denial-of-service attack where websites were flooded with service requests and their websites were overloaded and either slowed or crashed completely Writing or spreading computer viruses or worms
Intellectual property theft	Intellectual property theft including software piracy, and making and digitally distributing cyber/child pornography
Identity theft	Identity theft where this was accomplished by use of fraudulent computer transactions, such as collecting user ids and passwords using keylogger software
Harassment	Obscenities and derogatory comments at specific individuals focusing, for example, on gender, race, religion, nationality, and sexual orientation.

Table 4 shows the computer crime case distributions arranged by the six categories from 2003 to 2008. Figure 1 shows the distribution of cases based on computer crime types and years in a bar chart format. It helps show the most popular category as well as the number of cases for each category for each year.

Table 4: Computer Crime Cases by Category (2003-2008)

Computer Crime Category	2003	2004	2005	2006	2007	2008	Total
Fraud	1	4	1	7	9	9	31
Spamming	1	0	0	1	0	0	2
Hacking	3	4	8	5	8	6	34
Intellectual property theft	0	1	5	6	3	3	18
Identity theft	0	0	4	3	6	1	14
Harassment	3	1	0	0	0	2	6
Total	8	10	18	22	26	21	105

As shown in Table 4 and Figure 1, there was a sharp increase for the number of computer crime cases in the year 2005, compared to the previous years (i.e. 2003 and 2004). There were 18 cases reported by the newspapers in the year 2005, which was the total number of cases for the years 2003 and 2004. From the year 2006 onwards, there were over 20 computer crime cases reported in the newspapers. The top 2 computer crime types were fraud and hacking for the years 2007 and 2008.

There were also notable changes for individual types of computer crime cases. Figure 2 gives a clear picture of the changes occurred for each type. Fraud was the top 1 type from the year 2006 to 2008, and hacking climbed from the third place in the year 2006 to the second place in the years 2007 and 2008. Fraud went through a sharp increase from 1 case in the year 2005 to 7 cases in the year 2006 and continued the uptrend to 9 cases in the years 2007 and 2008

respectively. Intellectual property theft saw a up and down trend over the six years: from 1 case in the year 2004 up to 5 and 6 cases in the years 2005 and 2006 respectively; then down to 3 cases in the years 2007 and 2008.

Figure 1: Number of Cases by Crime Category (2003-2008)

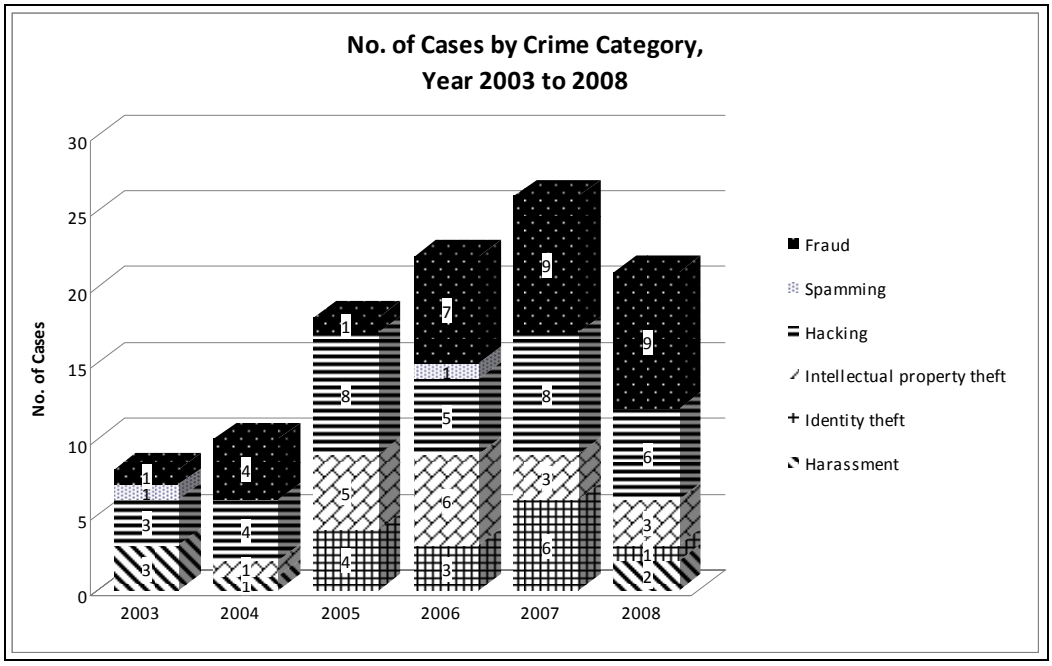
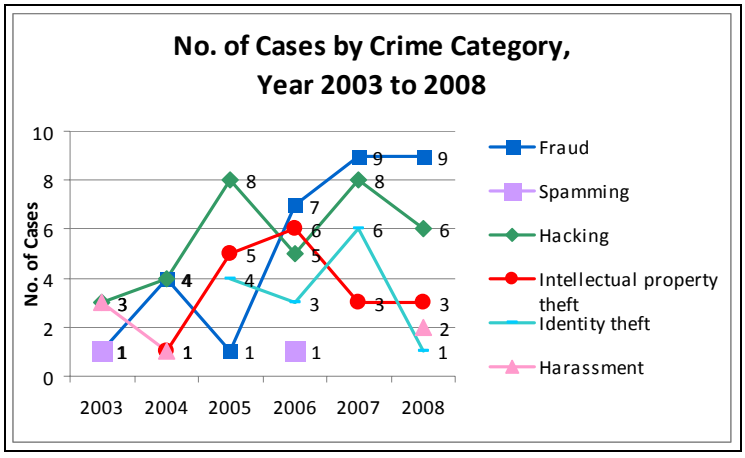
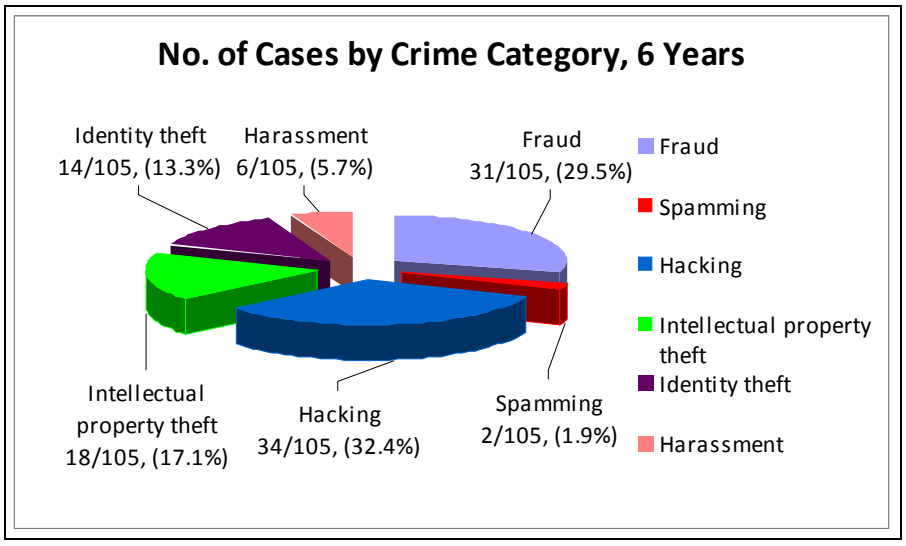


Figure 2: Year to Year Change in Number of Crime Cases



To show the most popular types over the six years, Figure 3 gives the details on the number of cases for each type as well as the percentage of each type over the six years. There were total 105 computer crime cases reported by the newspapers and the top 3 most popular types occupied 83 cases, or 79.0% of total cases. Among these 83 cases, hacking was the most popular type with 34 cases (32.4%), followed by fraud (31 cases, 29.5%), and intellectual property theft (18 cases, 17.1%).

Figure 3: Number of Cases by Crime Category (2003-2008)



From the collected computer crime cases, we identified the major crime tools: keylogger, phishing, card reader, and others. Table 5 shows the type of tools used in each crime category. For instance, the main tools used for fraud were phishing and card reader, and the tools for hacking were keylogger, phishing, and other tools such as Trojan horse programs.

Keylogger runs in the background on the victim's computer, and records all the keystrokes. Once keystrokes were logged, they were hidden in the machine for later retrieval, or shipped raw to the attacker. Phishing was the criminally fraudulent process of attempting to acquire sensitive information (such as user password) or make money illegally, by pretending as a trustworthy person mainly through e-mail. A card reader was a device used to scan cards containing magnetic data strips. It can be used to make a forged credit card by scanning the details of a credit card. Trojan horse programs contain

unexpected, additional functionality. For example, a bogus login script retains a copy of users' names and passwords for later, malicious use before passing them to the original server.

Table 5: Summary of Crime Tools used in Computer Crime

Crime Tools / Computer Crime Category	Keylogger	Phishing	Card Reader	Other Tools
Fraud	0	8	5	4
Spamming	0	1	0	0
Hacking	2	2	0	7
Intellectual property theft	0	0	0	1
Identity theft	4	1	0	3
Harassment	0	4	0	3
Total	6	16	5	18

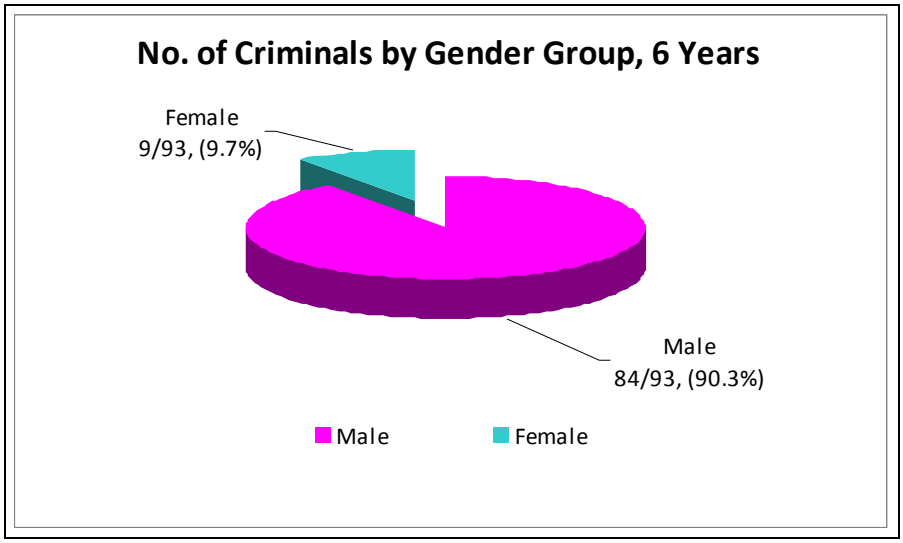
Table 6 showed sample computer crime cases in Singapore, which were listed under the corresponding computer crime categories.

Analysis on the characteristics of the criminals (or suspects) was done for gender, age, education, and occupation. Since some cases do not provide sufficient data, only the cases with required details were analyzed. There were 65 cases with criminal gender data over 105 cases and there was total 93 criminals' gender data collected from those 65 cases. Figure 4 describes the number of criminals by gender. For the years 2003 and 2004, there was no females identified; for the years from 2005 to 2008, there were some female criminals and the number was on the uptrend. Although there was increasing number of females, it was still a small portion of all criminals. Overall, 90.3% of criminals were male; females only occupied 9.7% over the six years. This result was in line with similar trends in Taiwan where males made up 81.1% of the computer criminals (Chen et al., 2005).

Table 6: Computer Crime Cases in Singapore

Category	Crime Cases
Fraud	- Local banks targeted by phishing e-mail bearing Monetary Authority of Singapore name to ask for confidential information - Two undergraduate students convicted of running a credit-card cloning syndicate - A former high-flier at DBS Nominees was jailed for three years after concocting a complex share selling scam that reaped him almost $200,000.
Spamming	- A local company that sent out unsolicited SMS messages to 300,000 cell phone users and then billed them $1 each was punished with a $150,000 fine. - A 15 years old boy (Primary 6) hacked into a portal system for electronic learning services and sent out 161,064 e-mail messages to one of his teachers, slowing down the e-mail service provided by the portal system.
Hacking	- Law Society and CapitaLand websites defaced respectively in 2006 and 2007 - A Polytechnic student piggybacked on neighbor's network and first to be charged with unauthorized wireless net access. - A young Chinese undergraduate on a scholarship to study in Singapore was accused of hacking into computers at his alma mater, Raffles Junior College, to see other students' grades.
Intellectual property theft	- A local interior design firm and a video games developing company were charged with using pirated software. - A business analyst from a local IT company was charged with selling mostly obscene movies. He posted messages on Yahoo! to advertise his pornography business and made copies of the movies on his laptop and desktop computers. - Two persons were charged with illegal music uploads by putting hundreds of songs on a net chat channel for people to download.
Identity theft	- A Myanmar student was jailed for stealing his fellow countrymen's IDs and passwords with spy software (Perfect Keylogger) and trying to steal the victims' money online. - A 27 years old man illegally accessed his former girlfriend's personal e-mail accounts and changed her password.
Harassment	- A Cisco manager sent defamatory e-mail saying a rival firm was facing bribery probe for his personal gain. - A civil servant was sentenced to 30 months' jail for sending hoax bomb messages to government websites. - An undergraduate student stole the passwords to several women's Internet Messenger accounts and told one of them that he would distribute doctored photographs of her unless she sent him her naked picture.

Figure 4: Criminals by Gender



We divided the criminals into four age groups: below 18, between 18 and 25, between 26 and 40, and above 40. There were 55 cases with criminal age data over total 105 cases and total 64 criminals' age data were collected from the cases. As shown in Figure 5, the top two age groups with most number of criminals were the age group between 26 and 40 and the age group between 18 and 25. They occupy 45.3% and 29.7% of all criminals respectively, and as a result 75% of criminals were at the age range from 18 to 40.

Compared to gender and age, there were less data for education and occupation of criminals. There were only 21 cases with criminal education data and 34 cases with criminal occupation data. Based on the cases with education and occupation data, we find that 73.9% of criminals have university or polytechnic education; 46.6% were at either management/professional or executive positions. Figures 6 and 7 give a detailed view of criminal data on education and occupation respectively.

Figure 5: Criminals by Age Group

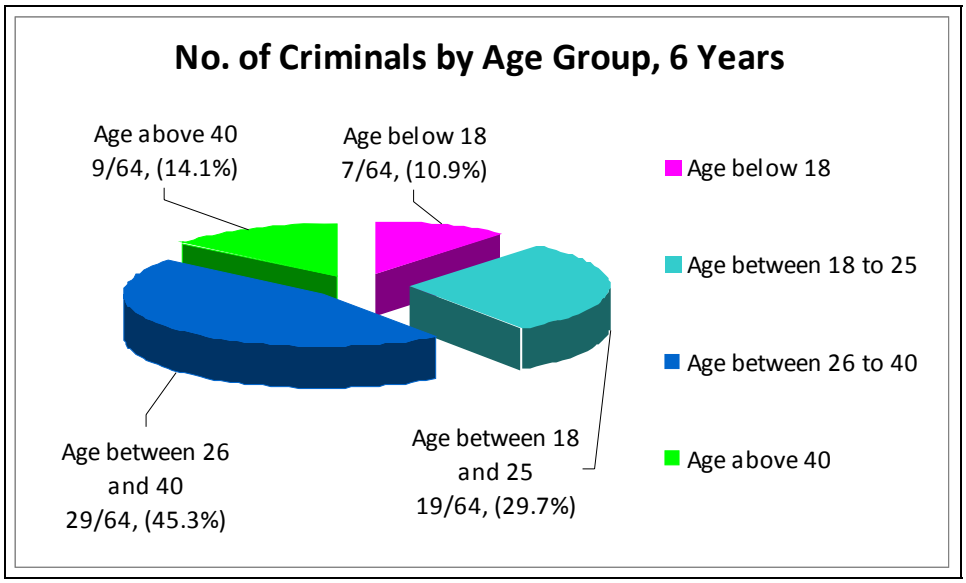


Figure 6: Criminals by Education Group

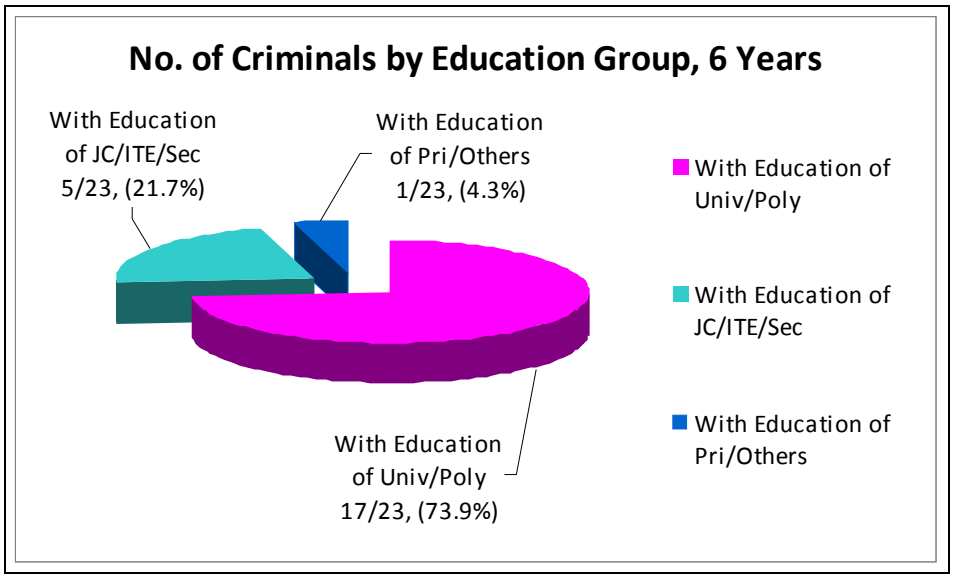
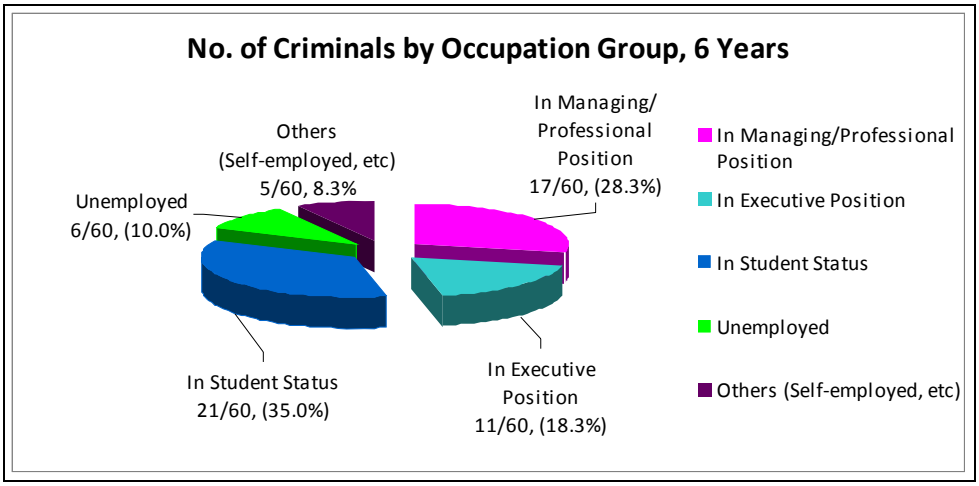


Figure 7: Criminals by Occupation Group

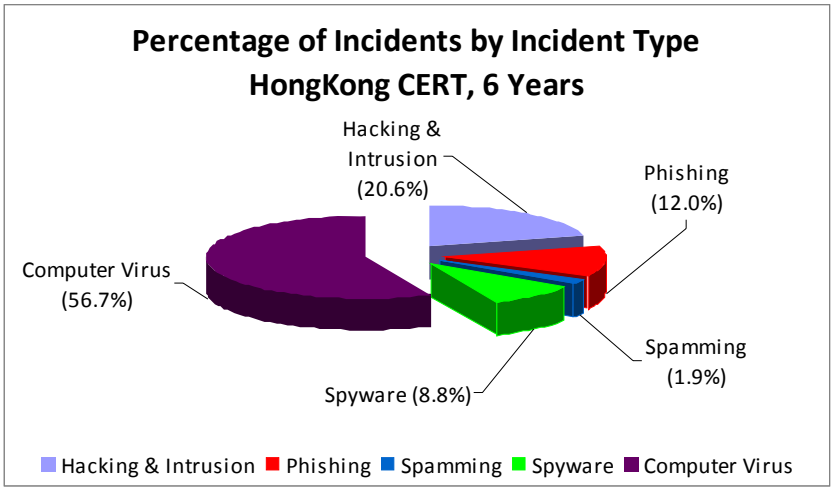


Computer Crime Trends in other Asian countries

We compared the computer crime trends in other four Asian countries with the one in Singapore. The four countries were Hong Kong, Malaysia, Thailand, and India. The data source was the annual reports from Asia Pacific Computer Emergency Response Team (APCERT; www.apcert.org). In the annual report for the year 2008, the response teams from the four countries provided the data on computer crime incidents from the year 2000 onwards to give an overview of the computer crime situations in these countries.

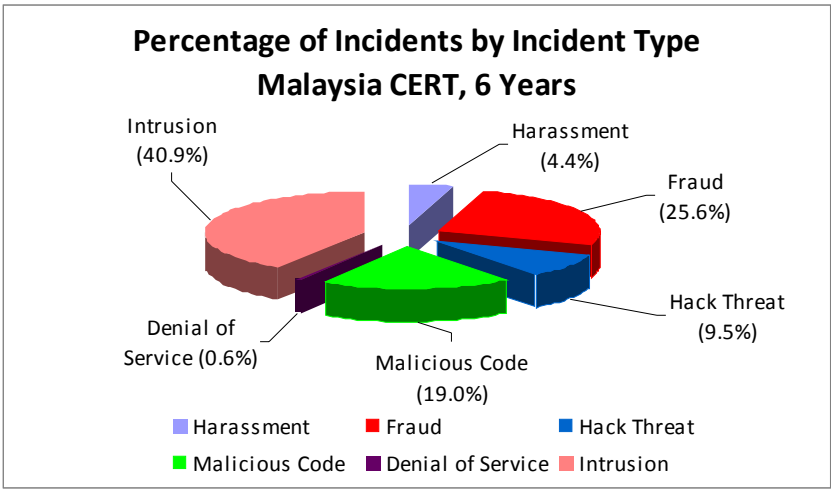
In Hong Kong, the number of computer crime incidents had been in a downward trend since the year 2005. The number of total incidents was reduced by 70% from the year 2004 to 2008. It suggested that computer crime in Hong Kong has gone into a slow track. Figure 8 showed that computer virus was the most frequent type which occupied 56.7% of all incidents over the six years, followed by hacking & intrusion (20.6%) and phishing (12.0%).

Figure 8: Computer Crime Incidents in Hong Kong



In Malaysia, the number of computer crime incidents had been steady until 2007, but showed a sharp upward trend in 2008. The types of incidents in an upward trend over the six years were harassment (267%), fraud (3240%), denial of service (240%), and intrusion (1277%). The other types (i.e. hack threat and malicious code) were in a downward trend. Figure 9 showed that the most frequent threat to Malaysia was intrusion, which occupied 40.9% of all incidents over the six years, followed by fraud (25.6%) and malicious code (19.0%).

Figure 9: Computer Crime in Malaysia CERT



In Thailand, the number of computer crime incidents had been in a downward trend since the year 2005. Compared to the other countries, there were much less incidents reported in Thailand. Figure 10 suggested that the most frequent threat to Thailand was malware, which occupied 41.6% of all incidents over the six years, followed by phishing (27.9%) and port scan and probe (18.5%).

Figure 10: Computer Crime Incidents in Thailand CERT

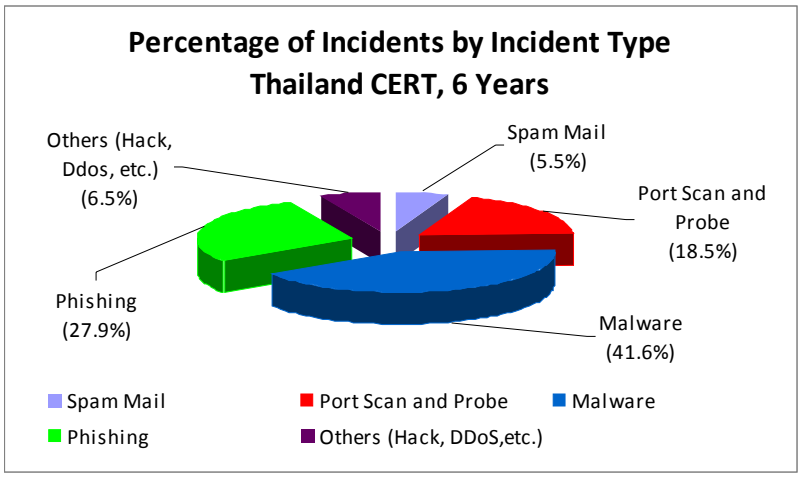
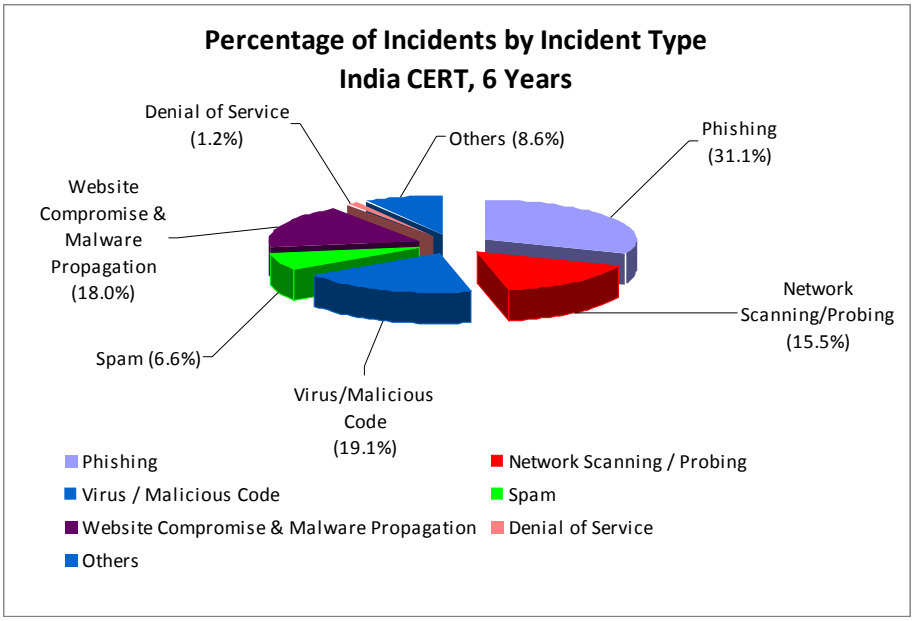


Figure 11: Computer Crime Incidents in India CERT



India CERT only started the incident data collection from the year 2004. In India, the number of computer crime incidents showed a sharp upward trend since 2004. Figure 11 showed that phishing was the most frequent incident type (31.1%), followed by virus/malicious code (19.1%) and website compromise & malware propagation (18.0%).

Table 7 showed the top three computer crime categories for Singapore, Hong Kong, Malaysia, Thailand, and India. Since different countries used different ways to categorize computer crime cases, it was not feasible to compare them directly, but we could see some similarities among them. Hacking and fraud were the two most popular computer crime categories in these five countries. It indicated that criminals were using computers not only to attack others' computers but also as a way to get illegal interests from others.

Table 7: Top 3 Computer Crimes 2003 to 2008 in 5 Countries

Country/ Region	1st crime category	2nd crime category	3rd crime category
Singapore	Hacking	Fraud	Intellectual property theft
Hong Kong	Computer Virus (Hacking)	Hacking & Intrusion (Hacking)	Phishing (Fraud)
Malaysia	Intrusion (Hacking)	Fraud	Malicious Code (Hacking)
Thailand	Malware (Hacking)	Phishing (Fraud)	Port Scan and Probe (Hacking)
India	Phishing (Fraud)	Virus / Malicious Code (Hacking)	Website Compromise & Malware Propagation (Hacking)

Findings and Discussion

Based on our data analysis on the collected computer crime cases in Singapore over the six years, there were some major findings.

Uptrend in Computer Crime Cases

FBI (Federal Bureau of Investigation) recently warned of the increasing trend of computer crime, which costs tens of millions of dollars and was threatening US security (NewsScientwast.com, 2008). According to the survey conducted by Computer Security Institute (CSI) in 2007 (Richardson, 2007), the actual number of computer crime cases could be much higher as only 29% companies reported the incident to law enforcement due to various reasons such as concern about negative publicity. Software nowadays claims more and more features and functions but behind it the complexities and vulnerabilities were increasing. CERT's vulnerability statistics shows a rising trend of software vulnerabilities from 1995 to 2008 although there was a small drop in 2007 (CERT, 2009).

In our study, we observed a dramatic increase on the number of computer crime cases reported by the newspapers, i.e. from 8 cases in 2003 to 18 cases in 2005 and to 26 cases in 2007. With the popularity of computers and the Internet, we anticipate a continuing rise in computer crime. Although there were a fewer cases in 2008 than 2007, the total number of computer crime cases still remained high. On the other hand, Yearbook of Statistics Singapore 2008 reported that overall crime (mainly traditional crime) rate had increased from 2002 to 2005, but there was a slight decline in recent years. For example, theft and related crimes dropped from 22,711 in 2005 to 19,522 in 2007 (Singapore Department of Statistics, 2008).

Fraud and hacking were Top Crimes in 2007 & 2008

More than 60% of cases fell into the types of fraud and hacking over the six years. Fraud was the number one crime type for the years 2004, 2006, 2007, and 2008. KPMG Singapore Fraud Survey Report 2008 (KPMG, 2008) reported that computer related fraud increased from 19% of total fraud in 2004 to 59% in 2007 and that computer related fraud had emerged as "the fastest

growing and most pervasive category of fraud" in the business world. This was due to the ever increasing reliance on technology by businesses.

Hacking was the number one crime type for the years 2003, 2004, and 2005, and the number two crime type for the years 2007 and 2008. Most hacking incidents were targeted at the computers of educational institutions, government agencies, and private sector. Based on the cases, the main motivation for hacking was revenge, self-pride or monetary purposes.

Intellectual Property Theft and Identity Theft Fluctuated

Intellectual property (IP) crime involves pirated computer software usage, especially by software development companies. IP crime reduced drastically after the implementation of the government's strong IP law in 2006 and the attractive incentive for employees who tipped off Business Software Alliance (BSA) about their companies using pirated software. In our study, cases for intellectual property theft increased from 1 case in the year 2004 to 6 cases in the year 2006, but decreased to 3 cases in the years 2007 and 2008 respectively.

The same situation also applied to identity theft: from 3 cases in the year 2006 to 6 cases in the year 2007, and the sharp reduction to 1 case in the year 2008. Identity theft usually involves using social engineering techniques such as phishing, and password stealing software such as keylogger. The Phishing Activity Trends Report (Anti-Phishing Working Group, 2006) reported that both phishing and keylogger have steadily increased usage from 2005 to 2006. This could be the reason for the proliferation of identity theft in the year 2007. There could be a few reasons for the sharp reduction to 1 case in the year 2008. In recent years, there have been stricter actions to prevent identity theft in order to create a better business environment in Singapore. Banks and organizations were also taking steps to put in place more measures to protect users' information, for example most banks in Singapore have implemented issuing thumb drives to their clients to obtain a secure pin before accessing their online banking services.

Most Criminals were Male and Aged 18 to 40

Over 90% of computer crime criminals (or suspects) were male. For the years 2003 and 2004, there was no females among the criminals with gender information. For the year 2008, although there were 4 female criminals, they were all non-main criminals. Based on the cases, we could see male criminals with various backgrounds, such as students, IT professionals, and managers. Young adults have mainly been involved in computer crimes as they have the essential skills.

Criminals had Higher Education with a Professional Career

From the computer crime cases, it was found that the criminals were degree holders and who had professional jobs. From the year 2003 to 2008, 73.9% of the computer crime cases were committed by university or polytechnic degree holders. 28.3% of the criminals were in management or professional positions, and 18.3% of the criminals had executive positions.

Conclusion

This study provided an overview of the current trend of computer crime in Singapore over the 6 years from 2003 to 2008. The findings from our analysis of computer crime cases indicated that the number of computer crime cases was in an uptrend over the six years. Fraud and hacking were the top two crime types, intellectual property theft and identity theft fluctuated over the six years, most criminals were male and in the age group between 18 and 40, and many criminals were well-educated and professionals. We also observed from related literature that Singapore had a good awareness of computer crime vulnerabilities and counter-measures, and the laws for computer crime were becoming more matured.

The main limitation of this study was the data sources since it was based on secondary data sources collected from the English language newspapers in Singapore. Firstly, due to the limited information being published in the newspapers, it was hard for us to get the full details of all the computer crime cases, such as computer tools, damage cost, age, occupation, and detailed methods. We probably missed some crime cases not reported on the

newspapers as well. In fact, newspapers cannot cover all the computer crime incidents, and companies do not want to report to the police as they think it will be bad publicity which seriously undermines the image and reputation of the companies, as well as public trust. If we could obtain accurate and detailed data from the local government agencies such as Singapore police force, Ministry of Home affairs, and Singapore Statistical department, we could produce a more reliable analysis. But there were some regulations and privacy policies on these organizations, so it was hard to get the data directly from them. In order to obtain more cases which were related to computer crime in Singapore, we may use other language newspapers, such as Chinese newspapers, in future work.

References

Anti-Phishing Working Group. (2006). *Phishing activity trends report*. Retrieved from http://www.antiphwashing.org/reports/apwg_report_june_2006.pdf

Attorney-General's Chambers. (2009). *Singapore Statutes Online*. Retrieved from http://statutes.agc.gov.sg/

Barton, P. & Nwassanka, V. (2003). Cyber-crime: Criminal offence or civil wrong? *Computer Law & Security Report, 19* (5), 401-405.

Bigelow, R. (1993). Computer security, crime and privacy in USA: A status report: Part IV: Privacy, *Computer Law & Security Report, 9*(2), 50-57.

Business Software Alliance (BSA). (2009). *Types of cybercrime*. Retrieved from http://www.playitcybersafe.com/cybercrime/

Byers, S., Rubin, A. D., & Kormann, D. (2004). Defending against an Internet-based attack on the physical world. *ACM Transactions on Internet Technology, 4* (3), 239–254.

Carr, I. & Williams, K. S. (2000). Securing the E-commerce environment: Enforcement measures and penalty levels in the computer misuse legislation of Britain, Malaysia and Singapore. *Computer Law & Security Report, 16* (5), 295-310.

Cerezo, A. I., Lopez, J., & Patel, A. (2007). International cooperation to fight transnational cybercrime. In *Proceedings of the Second International Workshop on Digital Forensics and Incident Analysis* (pp. 13-27), IEEE Computer Society, Washington, DC.

CERT. (2009). *CERT Statistics (Historical)*. Retrieved from http://www.cert.org/stats/

Chen, Y. C., Chen, P. S., Hwang, J. J., Korba, L., Song, R., & Yee, G. (2005). An analysis of online gaming crime characteristics, *Internet Research, 15* (3), 246-261.

Choudhury, A. R. (2009, January 1). Fresh challenges for IT security: Virtualisation, Web 2.0 to cut costs but will expose new vulnerabilities. *The Business Times.*

Chua, H. H. (2005, February 23). $38m plan to guard against cyber-terror: 24-hour monitoring centre will sound alert against hacking and other attacks. *The Straits Times.*

Chung, W., Chen, H., Chang, W., & Chou, S. (2006). Fighting cybercrime: A review and the Taiwan experience, *Decision Support Systems, 41* (3), 669-682.

Computer crime a growing threat, warns FBI. (2008, October 16). *New Scientist*. Retrieved from http://www.newscientist.com/article/dn14961

Endeshaw, A. (1999). Computer Misuse Law in Singapore. *Information & Communications Technology Law, 8* (1), 5-34.

Gwee, S. (2008, March 11). Caught in web of menace: Singapore has the second highest number of cyber-bullying cases after the US, says new survey. *The Straits Times.*

Hinduja, S. (2007). Computer crime investigations in the United States: Leveraging knowledge from the past to address the future. *International Journal of Cyber Criminology, 1* (1). Retrieved from http://ccrimejournal.brinkster.net/sameer.htm

John, J. (2006). *A Critical study of penal provisions of Singapore Computer Misuse Act*. Retrieved from http://ssrn.com/abstract=901902

KPMG. (2008). *Fraud: Prevent, detect, respond: KPMG Singapore Fraud Survey Report 2008*. Retrieved from http://www.kpmg.com.sg/publications/forensics_FraudSurvey2008.pdf

Luo, S. (2008, November 25). 40% rise in identity theft online: Report, jump in viruses to mine personal data, take control of computers: Microsoft. *The Straits Times.*

Newman, R. C. (2006). Cybercrime, identity theft, and fraud: Practicing safe Internet: Network security threats and vulnerabilities. In *Proceedings of the 3rd annual conference on Information Security Curriculum Development* (pp. 68-78), Kennesaw, GA.

Nigri, D. F. (1992). Investigating computer crime in the UK. *Computer Law & Security Report, 8* (3), 132-135.

Richardson, R. (2007). *CSI Survey 2007: The 12th annual computer crime and security survey*. Computer Security Institute. Retrieved from http://i.cmpnet.com/v2.gocsi.com/pdf/CSWASurvey2007.pdf

Singapore Department of Statistics. (2008). *Yearbook of Statistics Singapore*. Retrieved from http://www.singstat.gov.sg/pubn/reference/yos/yos2008.pdf

Sukhai, N. B. (2004). Hacking and cybercrime. In *Proceedings of the 1st Annual Conference on Information Security Curriculum Development* (pp. 128-132), Kennesaw, GA.

What is Cyber Crime? (2009). Cybercitizenship.org. Retrieved from http://cybercitizenship.org/crime/crime.html

About the Authors

Na Jin-Cheon, Assistant Professor, Wee Kim School of Communication & Information, Nanyang Technological University, Singapore

Email: tjcna@ntu.edu.sg

Wu Hao, Email: w070009@ntu.edu.sg

Ji Yong, Email: jiyo0001@ntu.edu.sg

Tay Mia Hao, Email: taym0016@ntu.edu.sg

Ramanathan Mani Kandan, Email: rama0036@ntu.edu.sg

Masters students, Wee Kim Wee School of Communication and Information, Nanyang Technological University, Singapore