Cybercrime & Cybercriminals: An Overview of the Taiwan Experience

ChiChao Lu
Center for General Education, Overseas Chinese Institute of Technology, Taiwan.
Email: chichao@ocit.edu.tw

WenYuan Jen*
Department of Information Management, Overseas Chinese Institute of Technology, Taiwan.
Email: denise@ocit.edu.tw

Weiping Chang, Shihchieh Chou
Department of Information Management, National Central University, Taiwan.
Email: {wpchang, scchou }@mgt.ncu.edu.tw

***Abstract*—This paper explores the increasing number of cybercrime cases in Taiwan and examines the demographic characteristics of those responsible for this criminal activity. The report is based upon data taken from the Criminal Investigation Bureau of Taiwan's cybercrime database over the interval of 1999 through 2004. The paper defines cybercrime, analyses cybercrime case statistics and examines profiles of cybercrime suspects' characteristics. The findings show that of all types of cybercrimes committed over the past six years, the top five are distributing messages regarding sex trading or trading sex on the Internet, Internet fraud, larceny, cyber piracy and cyber pornography. As for suspect characteristics, the findings show that 81.1% were male; 45.5% had some senior high school; 63.1% acted independently; 23.7% were currently enrolled students; and 29.1% were in the 18-23 age bracket, which was the majority group. For those enrolled student cybercrime suspects, the findings show that the percentage of junior high school and senior high school student suspects constituted 69.0% (2002), 76.1% (2003) and 62.7% (2004) of cybercrime suspects in their respective years. The high rate shows that the number of currently enrolled students suspected of involvement in cybercrime is cause for concern. Finally, this paper offers recommendations to governments, social agencies, schools, and researchers in their efforts to reduce cybercrime.**

***Index Term*—cybercrime, computer crime.**

I. INTRODUCTION

Cybercrime is becoming ever more serious, threatening personal, societal, and national security [19]. Many studies have noted that cybercrime also negatively impacts e-commerce [3, 7, 10, 11, 12]. An effort to raise public awareness of cybercrime cases and offenders' demographic characteristics would increase the likelihood that laws will be updated, that academic studies will be conducted and funded, and that industry will receive the financial incentive to further develop cybercrime detection tools.

Compilation of official cybercrime statistics in Taiwan was initiated in 1999. All cyber criminal records are sent to the Criminal Investigation Bureau (CIB), where the data is entered into a database. According to Taiwan police regulations, each cybercrime case is recorded on a criminal record form that contains information such as field event time and suspect's birth date, education, gender and vocation. This paper uses the CIB database as a window through which trends and changes in cybercrime between 1999 and 2004 might be clearly seen.

In recent years, the Internet has grown from an emerging technology to a 24-hour-a-day, 7-day-a-week source of services and information. With the growth in public access have come increasingly serious negative impacts on society. Cronan, et al. found that more than a third of business students (undergraduate and graduate) had misused computer system resources or software in their lifetimes [4]. Not only do students misuse computer systems, but some among them also commit cybercrime. Due to the rapid propagation of on-line games and gambling, cases of enrolled students getting caught in this net of illegal activity increase year after year. A review of cybercrime data would do much to clarify the current state of affairs and stimulate new law-making and research ideas.

This paper is organized as follows. First, cybercrime is defined and categories of cybercrime identified. Next, with reference to the Taiwan CIB database, detailed cases are discussed. Then, characteristics of cybercrime criminals and currently enrolled student cybercrime suspects are described. Finally, recommendations for future action are made. It is hoped that the findings of this paper might serve as a reference for cybercrime professionals, educational institutes, and government policy makers

II. CYBERCRIME

This paper is based on "Cybercrime in Taiwan - An Analysis of Criminal Records", by WenYuan Jen, Weiping Chang and Shihchieh Chou, which appeared in the *Proceedings of International Workshop, WISI 2006*, Singapore, April 9, 2006. Copyright 2006, Springer.

*Corresponding author. Tel: +886 4 27016855; Fax: +886 4 27075420

"Cybercrime" is generally defined as any illegal activity conducted through a computer. However, authorities disagree on where cybercrime takes place. Park defines cybercrime as any criminal activity employing an information system (which may not be computerized) as the channel through which it is committed [14]. In contrast, Philippsohn views cybercrime as transpiring mainly on the Internet [15]. The present study follows Thomas and Loader [20] in defining cybercrime as "illegal computer-mediated activities that often take place in the global electronic networks."

Cybercrime is a major problem faced by businesses attempting to establish and maintain an online presence [18], and cybercrime attacks can potentially be just as damaging to a nation's infrastructure as attacks by classical criminals. Wilson [22] cites the need to combat computer crime, cyber terrorism and information warfare on parallel paths. Development of effective security countermeasures for each and every type of attack are needed to control potential threats.

With a 64 percent annual growth rate in cyberattacks, cybercrime plays a primary role in hindering growth of e-commerce [16,17]. For instance, piracy in foreign countries has resulted in substantial losses to the U.S. motion picture industry, and threatens the industry's survival. The International Intellectual Property Alliance (IIPA) found that production rates of pirated optical disks in Taiwan have been among the highest in Asia for at least two decades [10]. The IIPA also reported these pirated disks resulted in an estimated loss of US$42 million for American firms. Is cybercrime so serious in Taiwan? The issue is indeed worthy of our attention.

III. THE CASES AND SUSPECTS OF CYBERCRIME IN TAIWAN

There are many types of cybercrime, including Internet fraud such as credit card and advance fee fraud, fraudulent Web sites, illegal online gambling and trading, network intrusion and hacking, virus spreading, cyberpiracy and cyberterrorismn, distributing child pornography, and identity theft [1]. The most common categories of cybercrime cross national and cultural boundaries. To increase domestic and international public awareness and to help people avoid becoming victims of cybercrime, cybercrime statistical reports may be examined. With reference to the Taiwan CIB database (1999-2004), this section explores the details of a number of cybercrime cases and suspects.

Table 1 summarizes the rapid growth seen in Taiwan's Internet user population [6] and the staggering growth in cybercrime cases and suspects for the years 1999 through 2004. We see that cybercrime cases and cybercrime suspects increased, over those five years, at an average annual rate 136.5% and 119.7% respectively. These changes have occurred during a period of time when overall population growth was nearly zero.

The Taiwan government deregulated the fixed network telecommunication market in 2001, resulting in rapid increase in Internet users and service providers. It should be noted that the numbers of cybercrime cases and suspects increased as some related broadband Internet applications such as online games and Internet cafés became fully accessible. Many young Internet users are avid fans of online games and related online entertainment. However, not all Internet users are the same. There are bad as well as good Internet users. Because, as telecommunications were deregulated, new Internet regulations were not clearly composed or widely communicated, many new types of criminal behavior, cybercrime, emerged.

Based on CIB cybercrime case data, Table 2 shows the top five types of cybercrime cases. The greatest number of cybercrime cases are money laundering (1999), cyber piracy (2000), spreading messages related to sex trading or trading sex on the Internet (2001, 2002), larceny (2003), and Internet fraud (2004). These are violations of the Control Act, Copyright Law, Child and Youth Sexual Prevention Act, Larceny and Fraud and Breach of Trust laws, respectively.

Both cyber pornography and spreading messages related to sex trading or trading sex on the Internet are listed in the top five cybercrime cases every year. Many suspects committed "Relations for Compensation" – a euphemism for prostitution. The term "Relations for Compensation" comes from the Japanese description of

Table 1. The overview of cybercrime cases and suspects in Taiwan

Year	Total Population	Internet Population	Number of Cases	Number of Suspects
1999	22,034,096	4,800,000	116	187
2000	22,216,107	6,260,000	427	516
2001	22,405,568	7,820,000	1,009	1,249
2002	22,520,776	8,230,000	3,118	3,740
2003	22,604,550	8,800,000	4,346	5,786
2004	22,689,122	9,160,000	5,633	7,306
Average Annual Growth	0.6%	14.3%	136.5%	119.7%

( ) stands for the numbers of enrolled student suspects

Table 2. The overview of top 5 cybercrime cases in Taiwan

Cybercrime case	1999	2000	2001	2002	2003	2004
Money Laundering	22.5%		5.6%			
Cyber pornography	16.0%	15.5%	8.9%	5.0%	4.7%	5.6%
Cyber piracy	13.4%	30.4%	15.9%	4.3%		
Spreading message of sex trading or sex trading	9.6%	20.0%	41.3%	33.8%	20.4%	22.6%
Internet fraud	9.1%	9.1%		13.3%	27.0%	49.2%
Gambling		4.7%				
Larceny			4.6%	32.0%	28.5%	1.7%
Against Personal Liberty					4.6%	
Computer misuse						12.2%
The percentage of the top 5 cybercrime case occupied	70.6%	79.7%	76.3%	88.4%	85.2%	91.3%

middle-aged men giving money or expensive gifts to young female students in return for sexual favors. It should be noted that many suspects in Taiwan were apprehended by police who posed as 'johns' in a special sting operation conducted in 2001 and 2002.

With the increased popularity of on-line games came an increase in the stealing of fictitious treasures and other assets. This stealing of fictitious treasure constituted about 30% of all cybercrime cases in 2002 and 2003. Criminal law was revised in 2003 to reclassify theft of this type as "Computer Misuse." In 2004, this reclassification resulted in a reduction of reported larceny cases to 1.7% and a 12.2% rate of this new class of "Computer Misuse" cases.

In 2004, Internet fraud cases accounted for half of all cybercrime cases. With the growth in Internet fraud cases, more Internet users have become increasingly aware of the potential dangers of making purchases over the Internet. The U.S. Federal Bureau of Investigation (FBI) and the Computer Security Institute (CSI) report that Internet fraud losses in the US alone were approximately $299 million [16]. Smith [17] pointed out that cybercrime directly affects consumers in negative ways, and that the cybercrime threat is a hindrance to e-commerce. The high growth of Internet fraud cases is of major concern.

IV. THE CHARACTERISTICS OF CYBERCRIME SUSPECTS

This study analyzes cybercrime suspects' records with regard to complicity, gender, student status, educational level, and age range. In order to illustrate the ratio of "cybercrime" to "total crime reported to the police" [13], this study lists their relationship in Tables 3,4, and 5. Results of the analysis follow.

Complicity

About 37% of cybercrime suspects acted as part of a group, and the most common crimes were Internet fraud, larceny, spreading messages regarding sex trading or trading sex, Internet gambling and cyber piracy. Although about 63% of suspects acted alone, in most of these cases the suspects committed spreading messages regarding sex trading or trading sex, larceny, Internet fraud, cyber pornography and cyber piracy. It is interesting to note that there have been no significant changes in the types of cases included among the five most frequent except in their ranking order.

Table 3. The overview of cybercrime in group, gender and student status in Taiwan

Year	Complicity		Gender		Student Status	
	Alone	Group	Male	Female	Non-Stu.	Student
1999	43.8%	56.2%	84.0%	16.0%	90.9%	9.1%
	(N/A)	*(N/A)*	(85.2%)	(14.8%)	(92.7%)	(7.3%)
2000	29.6%	71.4%	79.1%	20.9%	84.1%	15.9%
	(N/A)	*(N/A)*	(86.1%)	(13.9%)	(93.7%)	(6.3%)
2001	68.8%	31.2%	75.2%	24.8%	81.3%	18.7%
	(N/A)	*(N/A)*	(86.0%)	(14.0%)	(93.8%)	(6.2%)
2002	75.6%	24.4%	83.9%	16.1%	68.4%	31.6%
	(N/A)	*(N/A)*	(83.8%)	(16.2%)	(93.8%)	(6.2%)
2003	73.8%	26.2%	89.3%	10.7%	69.2%	30.8%
	(N/A)	*(N/A)*	(84.7%)	(15.3%)	(93.5%)	(6.5%)
2004	86.9%	13.1%	75.1%	24.9%	83.8%	16.2%
	(N/A)	*(N/A)*	(85.5%)	(15.5%)	(94.8%)	(5.2%)
1999-2004 cybercrime	63.1%	36.9%	81.1%	18.9%	76.3%	23.7%
1999-2004 Total crime	*(N/A)*	*(N/A)*	(85.2%)	(14.8%)	(93.7%)	(6.3%)

( ) stands for the percentage of total crime report to the police

In Table 3, we find that the number of cybercrime suspects in Taiwan who acted independently increased from 43.8% (1999) to 86.9% (2004). We believe these numbers might not be an accurate reflection of the actual situation. Because individuals conspiring to commit cybercrime might be physically located in different cities (or even countries) they might be inappropriately identified as acting alone. In another words, the lower rate (37%) of those acting in complicity might be inaccurate as complicity is difficult to detect. Hence, some cases of cybercrime identified as being independently perpetrated may actually be group perpetrated.

Gender

Table 3 shows that the majority of cybercrime suspects in Taiwan were male (81.1%). With a growth rate of 24.9% in 2004, the number of female suspects grew at a rate much greater than preceding years. In 2004, 1539 female suspects committed Internet fraud, seven times the number of female suspects (188) in 2003. Internet fraud and spreading messages regarding sex trading or trading sex are the top two types of cybercrime for male and female suspects respectively in Taiwan.

Student Status

We can also see from Table 3 that the number of currently enrolled students who committed cybercrime increased dramatically in 2002 and 2003, and approximately one-fourth of all suspects (23.7%) between 1999 and 2004 were currently enrolled students, most of whom were stealing virtual equipment and money from online games. The next most prevalent type of cybercrime was student suspects spreading sex trading messages on Internet. The large number of students involved in cybercrime is extremely serious, and all government agencies and educational institutes should devote more attention to this problem.

Education Level

Table 4 shows the distribution of Taiwan cybercrime suspects by education level. The majority of suspects held senior high school diplomas (45.5%); the second largest group was Bachelor's degree holders (27.8%); the third largest group was of junior high school graduates (17.9%), and other groups comprised the remaining 8.9%. For those suspects with senior high school educations, the proportion of larceny cases was higher than other cases. Among suspects with Bachelor's degrees, cases involving spreading messages regarding sex trading or trading sex

Table 4. The overview of education level of cybercrime suspects in Taiwan

Year	Elementary	J. High	S. High	College	Graduate School	Unlisted
1999	14.4% (13.7%)	12.8% (44.8%)	46.0% (30.7%)	25.1% (5.6%)	1.6% (0.4%)	0.0% (4.8%)
2000	1.7% (13.6%)	15.5% (43.9%)	41.9% (33.3%)	37.6% (7.4%)	1.0% (0.3%)	2.3% (1.5%)
2001	3.0% (13.8%)	17.4% (41.6%)	44.4% (34.2%)	33.0% (7.9%)	1.5% (0.3%)	0.6% (2.3%)
2002	1.4% (13.9%)	20.8% (38.1%)	47.4% (36.2%)	27.7% (8.8%)	1.6% (0.3%)	1.1% (2.8%)
2003	1.4% (11.9%)	23.1% (38.4%)	50.8% (38.2%)	21.6% (9.1%)	1.3% (0.3%)	1.8% (2.0%)
2004	9.6% (10.9%)	17.8% (38.8%)	42.5% (39.6%)	21.7% (8.9%)	1.8% (0.4%)	6.5% (1.4%)
1999-2004 cybercrime	5.3%	17.9%	45.5%	27.8%	1.5%	2.0%
1999-2004 Total crime	(13.0%)	(40.9%)	(35.4%)	(8.0%)	0.3%	2.5%

( ) stands for the percentage of total crime report to the police

were most prevalent. Among junior high school graduates, larceny was again the most widespread.

From 1999 to 2004, of the total crimes reported to the police, the greatest number were committed by those with elementary school, junior high school and senior high school educations. However, the vast majority of cybercrime cases were committed by junior high school, senior high school and college students. The differences between these two groups indicate that cybercrime is attracting the better educated to engage in criminal activities. For instance, suspects with elementary level education constituted only 5.3% of cybercrime suspects while they committed 13.0% of all crimes. On the other hand, only 8.0% of total crime suspects held Bachelor's degrees, yet college graduates accounted for nearly one fourth (23.7%) of all cybercrime.

Age Range

Among the age ranges shown in Table 5, the 18-23 age range accounted for the highest average percentage (29.1%) of cybercrime between 1999 and 2004, with the 24-29 age range (24.7%) second. The juvenile range and the 18-23 age range combined for a total of 44.8%, first among all ranges. As for the juveniles themselves, in the year 2003 they had the highest proportion (29.7%), and in 2002 were ranked second (27.8%). In the years after 2002, the percentage of cybercrimes committed by juveniles was much greater than the percentage of juvenile involvement in crime as a whole.

From 1999 to 2004, juveniles accounted for 3,664 cybercrime cases. Among these juvenile cases, the greatest number, 36.4% (1,333), were larceny cases; the second, at 19.3% (707), were Internet fraud cases, and third, at 10.3% (377) were cases of computer misuse. It may be that the above three types of cases are related to online gaming. In order to steal virtual property, criminals defraud Internet users or hack into victims' computers. With online game popularity blossoming in 2002, many young students became addicted to role-playing games where novices are easily cheated by experienced users. That juveniles committed cybercrime in order to get more virtual property when playing online games is hardly surprising. Unfortunately, some juveniles believed committing cybercrime did not actually harm anyone. As shown in Table 5, the years 2002 and 2003 had a higher proportion of both juvenile and 18-23 age group cybercrime suspects.

From Table 5, we see that in 2003 almost 30% of all cybercrime suspects were from the 18-23 age range; however, total crimes reported to the police were dominated by 30-39 age range suspects. According to the data in Table 5, the age range of cybercrime suspects was younger than that of suspects of total crimes reported to the police. For instance, from 1999 to 2005, juveniles committed a higher percentage of total cybercrime (15.7%) than of total crimes reported to the police (8.1%).

Table 5. The overview of age range of cybercrime suspects in Taiwan

Year	juvenile	18-23	24-29	30-39	40-49	50-59	60+
1999	6.0%	25.4%	29.5%	28.7%	7.5%	2.2%	0.7%
	(12.2%)		(18.1%)			(69.7%)	
2000	8.1%	26.6%	32.1%	24.2%	6.8%	1.2%	1.0%
	(10.3%)		(17.8%)			(71.9%)	
2001	9.8% (9.7%)	32.6% (15.4%)	30.4% (19.6%)	20.5% (27.9%)	5.3% (18.7%)	1.1% (6.0%)	0.3% (2.7%)
2002	27.8% (8.7%)	36.7% (15.1%)	18.7% (18.2%)	13.2% (26.6%)	2.5% (19.7%)	0.9% (7.6%)	0.2% (4.1%)
2003	29.7% (8.0%)	31.5% (14.8%)	19.7% (20.0%)	14.4% (27.2%)	3.9% (19.7%)	0.7% (7.3%)	0.2% (3.0%)
2004	12.6% (6.2%)	21.9% (12.6%)	17.8% (21.8%)	21.5% (28.6%)	13.7% (20.2%)	8.1% (7.6%)	4.4% (3.0%)
1999-2004 cybercrime	15.7%	29.1%	24.7%	20.4%	6.6%	2.4%	1.1%
1999-2004 Total crime	(8.1%)	(14.5%)	(19.9%)	(27.6%)	(19.6%)	(7.1%)	(3.2%)

( ) stands for the percentage of total crime report to the police

Table 6. The overview of enrolled student cybercrime suspects in Taiwan

Year	Elementary	J. High	S. High	College	Graduate School
1999	5.6% (1)	5.6% (1)	38.9% (7)	44.4% (8)	5.6% (1)
2000	1.2% (1)	8.5% (7)	25.6% (21)	62.2% (51)	2.4% (2)
2001	0.4% (1)	7.7% (18)	35.6% (83)	52.4% (123)	3.9% (9)
2002	0.9% (11)	23.7% (280)	45.3% (536)	28.6% (338)	1.4% (17)
2003	1.4% (24)	30.9% (550)	45.2% (805)	21.4% (381)	1.2% (21)
2004	1.4% (16)	23.6% (279)	39.1% (463)	33.7% (399)	2.2% (26)
1999-2004 cybercrime	1.8%	16.7%	38.3%	40.5%	2.8%

Suspects in the 40-49 age range accounted for a lower rate (6.6%) of cybercrime participation than adolescents, but the same group had a higher rate (19.6%) of total crime reports to the police. This may indicate that suspects in the 40-49 age range lack the computer knowledge necessary to commit cybercrime. The statistics reported in Table 5 show 44.8% of all cybercrime suspects were younger than 24. This is a clear indication that efforts to control cybercrime should be targeted toward youth.

V. THE NUMBER AND CHARACTERISTICS OF ENROLLED STUDENT CYBERCRIME SUSPECTS

As Table 5 shows, the juvenile range and the 18-23 age range combined for a total of 44.8% of all cybercrime cases from 1999 to 2004. However, in the considerable cybercrime literature, which often focuses on techniques and policies, numbers and characteristics of currently enrolled students committing cybercrime are seldom discussed. In order to inspire expanded research devoted to developing better policies and educational programs for campus students, this paper points out some serious results of Internet cybercrime.

The trend of enrolled student cybercrime suspects

Due to the innocence of young students and the fast propagation of on-line games and gambling, the Internet continues to attract many currently enrolled students and to ensnare too many of them in cybercrime activities.

Table 6 summarizes the growth seen in enrolled student suspects for the years 1999 through 2004. From 1999 through 2001, the majority of enrolled student suspects were college students. However, in the succeeding three years, the number of junior high school and high school students involved in cybercrime grew alarmingly and these younger students have displaced college students as leaders in cybercrime. In Table 6, we find that the percentage of both junior high school and high school student suspects constituted 69.0% (2002), 76.1% (2003) and 62.7% (2004) of cybercrime suspects. This high rate shows that the number of currently enrolled students suspected of involvement in cybercrime is cause for concern.

In 2003, the judiciary updated existing laws relevant to cybercrime. The latest law treats virtual property as "non-fixed assets." Hence, stealing virtual property from on-line games has not been considered theft since 2003. Rather, stealing virtual property is now considered "damaging electromagnetic records." Theft is a breach of criminal law, but cases of damaging electromagnetic records are considered civil cases to be brought to the courts only by lawsuit. Therefore, the number of enrolled student suspects has dramatically decreased except for college students and graduate students, whose cybercrime numbers continued to increase in 2004. It is clear that educational institutions must become actively involved in the effort to stop cybercrime.

The top three cases committed by enrolled student suspects

Generally speaking, the number of enrolled student cybercrime suspects continues to increase. Table 7 lists the top three types of cybercrime cases, which constitute approximately three-fourths of all student-committed cybercrime. In the years 1999-2004, theft and Internet fraud cases predominated among primary, junior high, and high school students. The primary factor may be that many enrolled student suspects are addicted to Internet on-line games and, perhaps, tempted into stealing other players' virtual property.

Spreading messages regarding sex trading or trading sex is the most frequently seen type of cybercrime among both undergraduate and graduate enrolled student suspects. This phenomenon is related to the "Relations

Table 7. The overview of top three cybercrime cases committed by enrolled student cybercrime suspects in Taiwan

Year	Elementary	J. High	S. High	College	Graduate School
1999 | 2004	1. Theft (38.5%)	1. Theft (37.7%)	1. Theft (35.2%)	1. Spreading message of sex trading or sex trading (38.3%)	1. Spreading message of sex trading or sex trading (50.7%)
	2. Internet fraud (21.2%)	2. Internet fraud (28.1%)	2. Internet fraud (21.3%)	2. Theft (17.4%)	2. Slander (17.3%)
	3. Spreading message of sex trading or sex trading (17.3%)	3. Spreading message of sex trading or sex trading (10.7%)	3. Spreading message of sex trading or sex trading (18.6%)	3. Internet fraud (15.0%)	3. Obscenity (9.3%)

Table 8. The overview of enrolled student suspects in group and gender in Taiwan

Year	Complicity		Gender	
	Alone	Group	Male	Female
1999	80.4%	19.6%	83.8%	16.2%
2000	66.0%	34.0%	91.9%	8.1%
2001	79.2%	20.8%	84.0%	16.0%
2002	73.1%	26.9%	89.0%	11.0%
2003	80.2%	19.8%	94.1%	5.9%
2004	81.3%	18.7%	92.4%	7.6%
1999-2004 cybercrime	76.7%	23.3%	89.2%	10.8%

for Compensation" activities mentioned earlier, where young men and women are paid in exchange for sexual services negotiated for over the Internet.

Complicity and gender

Table 8 shows that the majority (77%) of enrolled student cybercrime suspects in Taiwan acted independently, and that number is increasing slightly. According to the data presented in Table 7, the top three types of cases do not require advanced knowledge of technology; currently enrolled students are able to send sex trading messages, steal someone's virtual property or set up Internet fraud schemes very easily. The rate at which students act alone in committing cybercrime is higher than when all crimes are considered (63.1%; see Table 3). Enrolled student suspects may act alone because they are thinking only of picking up some extra spending money quickly and easily.

Table 8 also shows that the majority of cybercrime suspects in Taiwan were male (89.2%). This higher proportion of male enrolled student participation in cybercrime might be attributed to the fact that female enrolled students are probably more timid about committing unlawful acts.

VI. CONCLUSIONS

Based on cybercrime suspect records from 1999 to 2004, this study describes Taiwan cybercrime cases and suspects' characteristics as follows.

Cybercrime cases. In decreasing order, the top five types of cybercrime in Taiwan were spreading messages regarding sex trading or trading sex on the Internet, Internet fraud, larceny, cyber piracy and cyber pornography. Government statistics show that 44.8% of all suspects were younger than 24; hence, we can clearly see the need for more active measures to prevent young people committing cybercrime.

Among the top three types of cybercrime committed by enrolled student cybercrime suspects in Taiwan, cases committed by elementary, junior high school and senior high school enrolled students were primarily of Internet theft; in contrast, cases involving college and graduate school enrolled students were primarily of sex trading or spreading messages related to sex trading.

Suspect characteristics. Among all cybercrime suspects in Taiwan, 81.1% were male; 45.5% had a senior high school education level; 63.1% committed cybercrime alone; 23.7% were currently enrolled students; and 29.1% were in the 18-23 age range, which was the majority group.

Among all enrolled student cybercrime suspects in Taiwan, 76.7% committed cybercrime alone; 89.2% were male; 40.5% were currently enrolled college students (the majority group). In our portrait of young enrolled cybercrime suspects, the rate of elementary (1.8%), junior high school (16.7%) and senior high school (38.3%) student involvement totaled 56.8% of all student cybercrime. Judging from the growing rate of young enrolled cybercrime suspects, it is clear that the problem of cyberbrime among this group continues to escalate.

VII. RECOMMENDATIONS

This study proposes four recommendations to government agencies, social groups, schools and researchers.

Government. Both updating existing laws and enhancing specialized cybercrime task forces are needed [2]. To prevent cybercrime, government agencies have to revise out-of-date laws and recruit more qualified investigators. Basically, cybercrime criminals are unafraid of committing crimes in the cyberworld because relevant laws are less clear and enforcement is less stringent. More complete laws will help law enforcement officers fight cybercrime. Judicial decisions are influenced by soundness of evidence and the previous criminal record of the suspect. Hence, computer forensics labs need more investigators with technical and legal knowledge so that they might collect the digital evidence needed to successfully prosecute cybercrime.

Society. Goodman [8] pointed out that only 1% of computer intrusion cases are reported. Why do we see such a high percentage of unreported cybercrime? One reason is a lack of information security awareness, and another is the victims' desire to protect their reputations. Whiteman and Mattord [21] believe that information security awareness is important to information security. With high information security awareness, people will discover more cybercrime. After discovering cybercrime, people and companies should report it to authorities. If cybercrime cases continue to be ignored or unreported, successful attacks may tempt other criminals to repeat the crime. Hence, this study suggests that law enforcement agencies establish safeguards for the attacked companies or individuals. Ensuring victim anonymity will encourage others to come forward and report cybercrime.

Schools. In the past, students who committed cybercrime and were arrested by police told the courts that they didn't know what they had done was illegal. Students not only need to learn how to use computers but also should learn the basic laws related to computer use and about the ethical use of technological tools in the cyberworld. There is an urgent need for information ethics and ethical education programs, and more scholars, researchers and schools need to become involved. It is never too late to educate our students and other Internet users, regardless of their age.

Researchers. Scholars need to increase their research into the factors that lead to cybercrime and to discover methods of prevention. New information security tools that emerge from such advanced research will help us sift through the enormous volume of cybercrime related information and to prevent cybercrime's continued growth.

Cybercrime is excessively broad and inclusive of all types of crime. Each of us, in one way or another, is a potential victim. This study recommends that government agencies, legal professionals, schools and researchers work together against the growing cybercrime calamity. It is only with such coordinated effort that a safer cyberworld might be achieved.

ACKNOWLEDGEMENT

The authors would like to express their appreciation to the reviewers and the Editor-in-Chief for their helpful instruction and valuable comments on how to improve this paper.

REFERENCE

[1] H. Chen, W. Chung, J.J. Xu, G. Wang, Y. Qin, and M. Chau, "Crime data mining: a general framework and some examples," Computer, vol. 37, no. 4, pp. 50-56, 2004.

[2] W. Chung, W. Chen, and S. Chou, "An international perspective on fighting cybercrime," *Lecture Notes in Computer Science*, no. 2665, pp. 379-384, 2003.

[3] E.D. Cordy, "The legal regulation of e-commerce transactions," *Journal of American Academy of Business*, vol. 2, no. 2, pp. 400-407, 2003.

[4] T. P. Cronan, C. B. Foltz, and T. W. Jones. "Piracy, computer crime, and is misuse at the university," *Communications of the ACM*, 49(6):85-90, 2006.

[5] DS-MOI, Department Statistics, Ministry of the Interior (2005, January). "Annual population census," October 2005. [Online]. Available: http://www.moi.gov.tw/stat/index.asp

[6] FIND, Focus on Internet News and Data. "The statistics report of Taiwan Internet Users," October 2005. [Online]. Available: http://www.find.org.tw/ 0105/howmany/usage_1.asp

[7] D. Geer, "Security technologies go phishing," *Computer*, vol. 38, no. 6, pp. 18-21, 2005.

[8] M. Goodman, "Making computer crime count," *FBI Law Enforcement Bulletin*, vol. 70, no. 8, pp. 10-17, 2001.

[9] IIPA, "Special 301 report on global copyright protection and enforcement," *Washington DC: International Intellectual Property Alliance*, 303-322.

[10] K. F. McCrohan, "Facing the threats to electronic commerce," *The Journal of Business & Industrial Marketing*, vol. 18, no. 2/3, pp. 133-145, 2003.

[11] I. MacInnes, D. Musgrave, and J. Laska, "Electronic commerce fraud: towards an understanding of the phenomenon," In *2005 Proceedings of the 38th Annual Hawaii International Conference*, 2005.

[12] R. McCusker, "E-Commerce, Business and Crime: Inextricably Linked, Diametrically Opposed," *The Company Lawyer*, vol. 23, no. 1, pp. 3-8, 2002.

[13] Ministry of the Interior, "The statistics report of National Police Agency," October 2005. [Online]. Available: http://www.npa.gov.tw/stats.php

[14] D.B. Parker, Fighting *Computer Crime: A New Framework for Protecting Information*, Wiley Computer Publishing, 1998.

[15] S. Philippsohn, "Trends in Cybercrime - an overview of current financial crimes on the Internet," *Computers & Security*, vol. 20, no. 1, pp. 53-69, 2001.

[16] K. A. Saban, E. McGivern, and J. N. Saykiewicz, "A critical look at the impact of cyber crime on consumer internet behavior," *Journal of Marketing Theory and Practice*, vol. 10, no. 2, pp. 29-37, 2002.

[17] A. D. Smith, "Cyberciminal impacts on online business and consumer confidence," *Online Information Review*, vol. 28, no. 3, pp. 224-234, 2004.

[18] A. D. Smith, and W. T. Rupp, "Issues in cybersecurity: understanding the potential risks associated with hackers/crackers," *Information Management and Computer Security*, vol. 10, no. 4, pp. 178-83, 2002.

[19] N. B. Sukha, "Hacking and cybercrime," Proceedings of the 1st Annual Conference on Information Security Curriculum Development-ACM, pp. 128-132, 2004.

[20] D. Thomas, and B. D. Loader, "Introduction - Cybercrime: Law Enforcement, Security and Surveillance in the Information Age," In *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*. Taylor & Francis Group, New York, 2000.

[21] M. E. Whitman, and H. J. Mattord, *Management of Information Security*, Course Technology, Boston, 2004.

[22] C. Wilson, "Holding Management Accountable: A New Policy for Protection Against Computer Crime," In *National Aerospace and Electronics Conference, Proceedings of the IEEE 2000*, pp. 272-281, 2000.

Chichao Lu (chichao@ocit.edu.tw) is a Senior Lecturer in the General Education Center, Overseas Chinese Institute of Technology. He earned M.S. degrees in history at National Taiwan University and law at Tung Hai University. His research interests include cyber society and technology law.

WenYuan Jen (denise@ocit.edu.tw) is currently working as an Associate Professor at the Overseas Chinese Institute of Technology. She received her M.S. and Ph.D. from Texas A&M University in 1993 and National Central University in 2005, respectively. She has published papers in the *International Journal of Medical Informatics*, *Lecture Notes in Computer Science*, and *International Journal of Management and Enterprise Development*. Her research interests include cyber society and electronic commerce.

Weiping Chang (wpchang@mgt.ncu.edu.tw) is currently a doctoral candidate in the Department of Information Management at National Central University, Taiwan. He earned his Bachelor's degree from Central Police University in 1984 and his Master's degree in law enforcement administration from Western Illinois University in 1995. He was formerly the Director of Information System Office of the Criminal Investigation Bureau (CIB) of the National Police Administration in Taiwan. His research topics are knowledge management, information retrieval, and computer forensics.

Shihchieh Chou (scchou@mgt.ncu.edu.tw) is an Associate Professor of the Department of Information Management at National Central University. He received his PhD from Texas A&M University in 1984 with a major in computer and adult education. His research focuses on knowledge management,

information retrieval, software engineering and distance learning.