The Criminal Phenomenon on the Internet: Hallmarks of Criminals and Victims Revisited through Typical Cases Prosecuted

Xingan Li *

WITH THE GROWTH OF RESEARCH ON CYBERCRIME, increased attention has been given to the hallmarks of cybercriminals and the security levels of cybervictims by lawyers and law enforcement officials. The purpose of this study is to present an updated profile of cybercriminality and cybervictimization based on empirical methods. The study uses a sample of 115 typical cases prosecuted between 18 March 1998 and 12 May 2006, which were published on the official website of the United States Department of Justice. The study found that males are responsible for a majority of these cybercrimes. Cybercriminals are primarily between the ages of 17 and 45. Domestic perpetrators constitute the absolute majority of the cybercriminals. Outsiders are four times more likely to be involved in cybercrimes than insiders. Most cybercrimes did not involve monetary loss, while those that did caused an average of one million dollars in damage. The most vulnerable interests are in the private sector. The security measures taken by victims are surprisingly weak, and are vulnerable to uncomplicated cybercrimes. The punishments (both imprisonment and fines) for cybercrime are generally light.

AVEC L'ESSOR DE LA RECHERCHE SUR LA CYBERCRIMINALITÉ, les avocats et les responsables de l'application des lois accordent une attention accrue sur les indices des cybercriminels et des niveaux de sécurité des victimes de la cybercriminalité. L'objectif de cette étude consiste à présenter une mise à jour de la cybercriminalité et de la « cybervictimisation » fondée sur des méthodes empiriques. L'étude se sert d'un échantillonnage de 115 cas typiques ayant fait l'objet de poursuites entre le 18 mars 1998 et le 12 mai 2006, publiés sur le site Web officiel du Department of Justice des États-Unis. Selon cette étude, la majorité des cybercrimes sont commis par des hommes. L'âge des cybercriminels se situe en général entre 17 et 45 ans. Les contrevenants à l'échelon national constituent la majorité absolue des cybercriminels. Les contrevenants externes à l'organisation ont quatre fois plus de chance d'être impliqués dans des cybercrimes que les gens de l'intérieur. Les plupart des cybercrimes ne portaient pas sur des pertes d'argent, quoique ces crimes eussent entraîné des pertes moyennes d'un million de dollars. Les intérêts les plus vulnérables se retrouvent dans le secteur privé. Les mesures prises par les victimes pour assurer leur sécurité sont étonnamment faibles et exposées à des cybercrimes simples. Les sanctions (les peines d'emprisonnement et les amendes) imposées en cas de cybercrime sont en général assez légères.

* Faculty of Law, University of Turku, Finland

The Criminal Phenomenon on the Internet: Hallmarks of Criminals and Victims Revisited through Typical Cases Prosecuted

Xingan Li

1. INTRODUCTION

THE SOCIAL CHANGES OF RECENT DECADES HAVE BEEN PRIMARILY driven by the development of information and communications technology. One of the most significant negative impacts in this context is the emergence and rampancy of cybercrime. Research on criminal activity related to information and communications technology has become a focus of study in the fields of criminology, criminal law and information security.

Cybercrime is a comprehensive topic and attracts scholars from different disciplines. Many have written about the theoretical explanation for cybercrime. Studies of cybercrime have revealed different dimensions of this phenomenon. While the limited previous first-hand explorations have been widely accepted and cited, inconsistencies exist among various studies. Unfortunately, in the field of cybercriminal and cybervictim profiling, most subsequent theoretical treatises tend to reinforce the earliest findings, or at most provide some modest revisions.

It is critical to answer the following questions: Who is most likely to commit cybercrime? Who is most likely to be victimized by cybercrime? And what are the similarities between cybercrime perpetrators and their victims? The subject of cybercrime leads the tide of the theory and practice of legislation and law enforcement in the sense that the perpetrators are those who challenge the traditional legal system. Studies on the subject of computer crime have a history of several decades and have established widely-accepted profiles for cybercriminals and their victims.

With the deepening of the research on cybercrime, lawyers and law enforcement officials are paying increased attention to the hallmarks of cybercriminals and the security of cybervictims. The purpose of this study is to present an updated profile of cybercriminality and cybervictimization, through the analysis of 115 typical cybercrime cases prosecuted in the United States of America between 18 March 1998 and 12 May 2006, and published on the Department of Justice website.

*

2. LITERATURE REVIEW

WHEN WE TALK ABOUT SUBJECTS OF CYBERCRIME, we are referring to the profile of the perpetrators of these crimes. However, the cybercriminal is not one single person, but represents a class of perpetrators. Previous literature has focused on who is most likely to commit cybercrime and who is most likely to be a victim of cybercrime. Any conclusions drawn from the hundreds or thousands of cases might be premature or even misleading. More than 20 years ago, Bequai pointed out that no one single profile could be developed of a cybercriminal.[1] Bequai offered a tentative profile of the typical perpetrator of computer crime based on hundreds of cases compiled from statistics by the United States Bureau of Justice.[2] Like many scholars, he was worried that attempts to oversimplify the profile of cybercriminals could have a misleading effect on our understanding of cybercrime. Bequai states that:

> Studies of computer criminals usually portray them as young, educated, technically competent, and usually aggressive. Some steal for personal gain, others for the challenge, and still others because they are pawns in a larger scheme. … Still other studies typically portray computer criminals as technicians, managers, and programmers. They are usually perceived as jovially challenging the machine, and discovery occurs only through inadvertence. … The theft usually involves money, services, or trade secrets. However, when caught, the computer criminal's sentence is light compared to that of traditional property-crime felons, who usually receive harsh sentences for crimes involving much less property or money.[3]

It is widely recognized that there is no single profile that can "capture the characteristics of a 'typical' computer criminal, and many who fit the profile are not [necessarily] criminals at all."[4] Donn B Parker presented a brilliant portrait of a perpetrator of computer crime, stating that "[p]erpetrators are usually bright, eager, highly motivated, courageous, adventuresome, and qualified people willing to accept a technical challenge. They have exactly the characteristics that make them highly desirable employees in data processing."[5]

The development of computer technology has changed this depiction completely.[6] Becker suggested seven views of computer systems: the playpen, the land of opportunity, the cookie jar, the war zone, the soapbox, the fairyland, and the toolbox.[7] Bequai researched how the potential sources of computer attack might vary from one to another, and found that the majority of perpetrators could essentially be grouped into three categories: dishonest insiders; outsiders; and users.[8] This implied that everyone had an equal chance of being involved in

1. August Bequai, *How to Prevent Computer Crime: A Guide for Managers* (John Wiley & Sons., 1983) at p. xviii.
2. Bequai, *How to Prevent*, *supra* note 1 at pp. 42-45.
3. August Bequai, *Computer Crime* (Lexington Books, 1978) at p. 4.
4. Charles P Pfleeger and Shari Lawrence Pfleeger, *Security in Computing,* 3d ed., (Prentice Hall, 2003) at p. 20.
5. Donn B Parker, *Crime by Computer* (Charles Scribner's Sons, 1976) at p. 45.
6. Jay Becker, "Who are the Computer Criminals," (1981) 25:1 *Security Management* 18–22.
7. Becker, "Computer Criminals," *supra* note 6 at pp. 18–20.
8. Bequai, *How to Prevent*, *supra* note 1 at pp. 47–50.

computer crime, at a time when the internet was not as widespread as it is presently. Wasik concentrated on the characteristics and classifications of perpetrators as well.[9] Levinson sorted categories of cyber threats into five groups: insiders, hackers, virus writers, criminal groups, and terrorists.[10] Reynolds classified perpetrators into hacker, cracker, insider, industrial spy, cybercriminal and cyberterrorist.[11] That is to say, the widespread use of computers created a multi-dimensional social environment that allowed potential computer criminals to discover new opportunities for attack.

Internet users worldwide are strongly sex divided; that is, a higher percentage of males than females use the internet. For example, in 2001, women made up 6 percent of internet users in the Arab states, 38 percent in Latin America, 25 percent in the EU, 37 percent in China, 19 percent in Russia, 18 percent in Japan, 17 percent in South Africa, and nearly 50 percent in the United States.[12] However, the gender gap is narrowing, with females constituting the majority of internet users in some countries. In Nordic countries, it was found that men constitute a higher percentage of daily users of the internet than women.[13] Previous studies showed that cybercrime is far more sex divided than internet use. According to Levinson, "[i]t is well established that boys commit far more juvenile crime, particularly violent crime, than girls."[14] Cybercrime seems less violent, but the research indicates that more males commit cybercrimes than females. According to Jiang, males constitute 91.45 percent of the perpetrators, while females constitute only 8.55 percent.[15] He suggested that this was the result of differences between males and females in computer knowledge and skills combined with attitudes in online interactions. However, the reasons why females are found guilty of cybercrime less often than males are not clear at all. Specific research is needed to address the following questions: Do women commit less cybercrime? Are cybercrimes committed by women less likely to be detected? More philosophically, can we measure this criminal phenomenon among men and women using the same concept? But this study is not intended to answer these questions.

A noteworthy phenomenon is that whether it be individual cybercrime, corporate cybercrime, or organized cybercrime, young perpetrators play a critical part. Although there is no age limit to commit cybercrime, we found that, similar to traditional crimes, youth constitute an important proportion of the cybercriminals. As LR Shannon reported, in 1993, cybercriminals tend to be between the ages of 14 and 30; they are usually bright, eager, highly motivated, adventuresome and willing to accept technical challenges.[16] The age of criminal responsibility varies from nation to nation. In most countries, children younger

9. Martin Wasik, *Crime and the Computer* (Oxford University Press 1991) at pp. 60–65.
10. David Levinson, ed., *Encyclopedia of Crime and Punishment*, vol. 2. (Sage Publications, 2002) at p. 525.
11. George Reynolds, *Ethics in Information Technology* (Thomson Course Technology 2003) at pp. 58-65.
12. Women's Learning Partnership, "Technology Facts & Figures," (December 2001), <http://www.learningpartnership.org/resources/facts/technology>.
13. Nordic Council of Ministers, "Nordic Information Society Statistics 2005," Report, <http://www.norden.org/pub/uddannelse/IT/TN2005562.pdf> at p. 42.
14. Levinson, *Encyclopedia*, *supra* note 10 at p. 490.
15. Ping Jiang, *A Study of Computer Crime* (Shang wu yin shu guan, 2000) at pp. 151–152.
16. LR Shannon, "The Happy Hacker," review of Paul Mungo and Bryan Clough, Approaching Zero: The Extraordinary Underworld of Hackers, Phreakers, Virus Writers, and Keyboard Criminals (Random House, 1993), (21 March 1993) *The New York Times* G 16, <http://query.nytimes.com/gst/fullpage.html?res=9F0CE1D71E3BF932A15750C0A965958260>.

than 14 or 15 years of age are not liable for criminal offences, while children between 15-17 or 14-16 years of age are liable for a limited range of offences.[17] In fact, juveniles commit a number of these crimes. In China, individuals between the ages of 19 and 40 make up 80 percent of all internet users, and the average age of cybercrime perpetrators is 23.[18] Juvenile delinquency and juvenile justice have become issues closely associated with cybercrime. According to findings of criminal psychological research, the reason why children are more likely to commit crime is not because more and more children will commit crime, but because most of the potential offenders will commence to commit crime in childhood and continue their criminality for much of their lifetime. After 16-17 years of age, the offending rates decreases to a plateau.[19]

Underwood found that cybercriminal behaviour cuts across a broad range of society, with the age of most offenders ranging from 10 to 60 years.[20] People between the ages of 20 and 59 make up 94 percent of computer criminals, with the most active being people in their thirties.[21]

Bequai's profile of typical computer criminal presented a full portrait of the above mentioned features, with other aspects.[22] He stated that the age of computer criminals is between 15 and 45 years old. He found that males were responsible for most computer crimes, but that the proportion committed by females was increasing. The occupational experience of computer criminals ranged from the highly experienced technician to the minimally experienced professional. Both public and private sectors could be victims of computer crimes. Computer criminals had the personal traits of being bright, motivated, and ready to accept technical challenges. They were usually desirable employees who were hard and committed workers. Computer crimes were mostly committed by individuals, but conspiracies were increasing. Most offences were committed by insiders who had easy access to the computer system. The security of the victims' system was usually lax.

An important topic of research has been the distinction between the sources of offenders and the relationship between offenders and their victims, which can be used to divide offences into those committed by insiders and those committed by outsiders. Shaw, Ruby and Post classified insiders into information technology specialists such as full-time or part-time employees, contractors, consultants, or temporary workers; partners and customers with system access; and former employees retaining system access.[23] There have been different findings as to whether insiders or outsiders constitute the greatest threat to computer system security.[24]

---

17. For example, in Article 17 of the penal law of China, children under 14 years old of age are not liable; in Section 4, Chapter 3 of the Penal Code of Finland, <http://www.finlex.fi/pdf/saadkaan/E8890039.PDF>, the age limit is 15. In some other countries, the liability age is even lower. In England and Wales, the age is 10-year-old, while the limited liability ages are between 10-14 years of age.
18. B Dong, "Eighty Percent of Net Café Consumers are Youths," (15 October 2003) *China Youth Newspaper*
19. Dennis Howitt, *Forensic and Criminal Psychology* (Prentice Hall, 2002) at pp. 76–77.
20. Jim Underwood, "Criminal Profile," (1999), <http://www-staff.it.uts.edu.au/~jim/cit2/cit2-99/legal/CrimProf.html>
21. Jim Underwood, "Criminal Profile," *supra* note 20.
22. Bequai, *How to Prevent*, *supra* note 1 at p. 43.
23. Eric D Shaw, Keven G Ruby, and Jerrold M Post, "The Insider Threat to Information Systems," (1998) 2-98 *Security Awareness Bulletin*, <http://rf-web.tamu.edu/security/secguide/Treason/Infosys.htm>.
24. For example, The AFCOM's Data Centre Institute found that the cyber attacks launched by outsiders (52 percent) were ten times that of the insiders (5 percent). However, the respondents were more concerned the insider threats than the outsider ones. See Edward Hurley, "Are Insiders Really a Bigger Threat?" (17 July 2003), <http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci906437,00.html>.

Mainstream findings support the view that insiders are more likely to be involved in computer crimes against the employers' systems. The Nordic Council of Ministers found that students, employees and self-employed people constitute the highest percentage of internet users.[25] Mackenzie and Goldman reported that "some students, particularly computer science and engineering majors, with newly discovered skills attempt to break into the servers" of University of Delaware.[26] In November 2003, Meta Group found that, of more than 1,600 information and communications technology professionals, current employees represent the biggest threat to technology infrastructures.[27] The Computer Security Institute and Federal Bureau of Investigation found that 55 percent of survey respondents reported malicious activity by insiders.[28] Researchers also revealed that dissatisfied employees are a major source of computer crimes[29] and are the greatest threat to a computer's security.[30] When Sutherland coined the term "white-collar crime" in the late 1930s, he could have hardly imagined that crimes would be committed in the process of human-machine interaction, in addition to human-human interaction, human-organization interaction, or human action against machines. Nevertheless, the term "white-collar cybercrime" was recently introduced as a contribution to develop Sutherland's theory.[31]

Besides the revealed relationship between criminals and victims, others have also explored the characteristics of victims. Debra Littlejohn Schinder suggests a summary of common cybervictim characteristics: they are new to the internet; naturally naïve; disabled or disadvantaged; greedy; lonely or emotionally needy; pseudo-victims in the sense that they may falsely report being victimized; or are simply unlucky enough to be in the wrong virtual place at the wrong time.[32]

From the previous literature, the profile of the cybercriminal and the cybervictim can hardly be regarded as settled. In addition, the available literature does not provide detailed sources of materials nor does it clarify the methods used. Many studies have apparently been based on second-hand materials and mass media reports. There is still a need for findings about the hallmarks of cybercriminals and cybervictims drawn from the prosecuted cases.

---

25. "Nordic Information Society Statistics 2005," *supra* note 12 at p. 42.
26. Elizabeth MacKenzie and Kathryn Goldman, "Computer Abuse, Information Technology, and Judicial Affairs," in *Proceedings of the 28th Annual ACM SIGUCCS Conference on User Services: Building the Future* (ACM Press, 2000) 170–176 at p. 174.
27. Meta Group, "Security Spending Spree," (20 January 2004) 23:1 *PC Magazine* 25.
28. Bill Hancock, "Security Views," (1999) 18:3 *Computers and Security* 188-189.
29. Michael A Vatis (Director, National Infrastructure Protection Center, Federal Bureau of Investigation), Statement for the Record, *NIPC Cyber Threat Assessment*, hearing, Senate Judiciary Committee Subcommittee on Technology and Terrorism, 106th Congress, 1st session (USA, 6 October 1999) at "Insider Threat."
30. Eric J Sinrod and William P Reilly, "Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws," (2000) 16:2 *Santa Clara Computer and High Technology Law Journal* 177–232 <http://www.sinrodlaw.com/CyberCrime.pdf>.
31. See for example, Victim Assistance Online, "White Collar Cybercrime," <http://www.vaonline.org/internet_wcollar.html>. The term "White-Collar Hacker" is also used, for example, by John Leyden, "The Rise of White Collar Hacker," (31 March 2004) *The Register*,<http://www.theregister.co.uk/2004/03/31/the_rise_of_the_white/>.
32. Debra Littlejohn Shinder, *Scene of the Cybercrime: Computer Forensics Handbook* (Syngress Publishing, 2002).

*

3. METHODS

THE STUDY USED A SAMPLE OF 115 TYPICAL CASES sentenced or on trial between 18 March 1998 and 12 May 2006 published on the website of the United States Department of Justice. The study took all the cases listed on the website of the United States Department of Justice Computer Crime & Intellectual Property. The webpage notes: "Below is a summary chart of recently prosecuted computer cases. Many cases have been prosecuted under the computer crime statute, 18 U.S.C. §1030 [(2000) 18 *United States Code* s. 1030, <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+18USC1030>]. This listing is a representative sample; it is not exhaustive."[33]

The study classified the sample cases as follows: hacking and illegal access; attack, sabotage and botnet; viruses, worms, spyware and logic bomb; data theft and espionage; ID theft and fraud; and miscellaneous, which includes embezzlement and corruption. The strict legal categorization is not used in this study. Rather, the classification is based on criminological characteristics of the behaviours.

The statistical items considered in this study include: the demographic characteristics of the cybercriminal (including gender, age, insider or outsider, American citizen or foreigner); the nature of the victims (including private, public, both private and public, and threat to public health or safety); the outcomes of the cases; the decided sentence for the cybercrime (imprisonment and fine), the level of security of the victim (classified into strong, medium, and weak); and the complexities of techniques involved (classified into complicated, medium, and simple).

*

4. RESULTS

4.1. Gender Distribution of Cybercrime

IN MOST CATEGORIES OF OFFENCES, MALE OFFENDERS constitute the absolute majority of the criminals. Only two female offenders are reported in hacking and illegal access and one female offender is reported in miscellaneous offences. Overall, male offenders constitute more than 98 percent of the total perpetrators, while females are less than two percent.

4.2. Age Distribution of Cybercrime

The report from the website is incomplete in providing offenders' age information in every category of offence. Age data is missing for 73.1 percent of ID theft offences; 30.4 percent of attack, sabotage and botnet offences; 18.2 percent of viruses, worms, spyware and logic bomb offences; 15.9 percent of hacking and illegal access offences; 14.3 percent of data theft and espionage offences; and 14.3 percent of miscellaneous offences.

---

33. United States Department of Justice, Computer Crime & Intellectual Property Section, "Computer Crime Cases," <http://www.cybercrime.gov/cccases.html>.

Three perpetrators younger than 16 years old were convicted of offences in the categories of hacking and illegal access, and viruses, worms, spyware and logic bomb.

Offenders in the age category older than 46 years old were found in all categories of offences, except for fraud and miscellaneous offences. Generally, offenders over the age of 46 years old are not active in computer crime and constitute a small percentage of the total reported offenders, including offences for which ages are not available. For example, offenders over the age of 46 years old were convicted for 28.6 percent of data theft and espionage offences; 9.1 percent of virus, worms, spyware and logic bomb offences; 4 percent of attack and sabotage offences; and 3.8 percent of ID theft offences.

Cybercriminals are primarily between the ages of 17 to 45 years old. Offenders in this age group committed 79.3 percent of crimes involving hacking and illegal access; 65.2 percent of those involving attack and sabotage; 63.7 percent of those involving viruses, worms, spyware and logic bombs; 85.8 percent involving data theft and espionage; 26.8 percent involving ID theft; 100 percent involving fraud; and 85.7 percent that can be categorized as miscellaneous.

A more detailed distribution of offenders between the ages of 17 and 45 years old can be described as follows: the number of the offenders between the ages of 17 and 25 is 41; the number between 26 and 35 is 39; and the number between 36 and 45 is 21. These categories constitute 27 percent, 26 percent, and 17 percent of all offenders respectively. In the age group of 17 to 45 years old, 17 to 25-year-olds constitute 40.6 percent; 26 to 35-year-olds 38.6 percent; and 36 to 45-year-olds 20.8 percent. The ratios of offenders seem to decrease with age.

4.3. Domestic Versus Foreign Perpetrators

Altogether 14 out of 115 cases, or less than 12.2 percent, were committed by international perpetrators or foreigners. Domestic perpetrators are responsible for the remaining 87.8 percent of cybercrimes. The majority of reported cases are domestic computer offences.

4.4. Insider Versus Outsider

Insiders and outsiders constitute different ratios in different categories of offences. Insiders constituted the majority of offenders for offences of data theft, espionage, and fraud.

The categories in which outsiders constitute the majority of offenders include: exactly 100 percent of ID theft offences; 92.9 percent of miscellaneous offences; 87 percent of attack, sabotage and botnet offences; 81.8 percent of viruses, worms, spyware and logic bomb offences; and 76.2 percent of hacking and illegal access offences. Outsiders also constitute a strong ratio of 42.9 percent in fraud offences.

Former employees are included in the category of outsiders. Former employees make up 43.5 percent of offenders of attack and sabotage. They also constitute 12.7 percent of offenders of hacking and illegal access, and 7.2 percent of offenders of miscellaneous offences.

Overall, insiders and outsiders constitute 21 percent and 79 percent of all reported offenders respectively. Former employees constitute 16 percent of all of the outsiders. If former employees are added to insiders, they would constitute about 34 percent of the total offenders, still a smaller ratio than outsiders.

4.5. Losses Resulting From Cybercrime

In more than 59 percent of cybercrime cases, no loss was mentioned in the report. Among the remaining 41 percent of cases, 7 percent report losses of less than 10,000 dollars; 15.7 percent report losses between 10,000 and 100,000; 10.4 percent report losses between 100,000 and one million dollars; and 9.6 percent report losses of more than one million dollars.

The cybercrime offences with the greatest losses were hacking and illegal access; viruses, worms, spyware and logic bomb; ID theft; and miscellaneous offences, each resulting in losses of over one million dollars. The average losses resulting from attack and sabotage, data theft and espionage, and fraud are relatively lower: USA$160,000, USA$5,000 and USA$384,000, respectively.

Overall, the average loss of the reported 49 cases is USA$2.989 million. Adding cases without losses reported, the average loss still reaches USA$1.274 million.

4.6. Victims of Cybercrime

The private sector is the primary victim of cybercrime. All of the cases of data theft and espionage, ID theft, and fraud are against private interests. 87.5 percent of miscellaneous offences, 81.8 percent of viruses, worms, spyware and logic bomb offences, 77.3 percent of attack and sabotage offences, and 69.5 percent of hacking and illegal access offences are committed against the private sector.

Only 18.2 percent of attack and sabotage offences, 13.6 percent of hacking and illegal access offences, and 12.5 percent of miscellaneous offences are committed against the public sector. However, 15.3 percent of hacking and illegal access cases and 9.1 percent of viruses, worms, spyware and logic bomb cases are against both private and public sectors.

In addition, 9.1 percent of viruses, worms, spyware and logic bomb cases, 4.5 percent of attack and sabotage cases, and 1.7 percent of hacking and illegal access cases are against public health and safety interests.

4.7. Security Level of the Victim

In the majority of cases, security is weak. Exactly 100 percent of cases of data theft and espionage and ID theft are possibly due to the absence of appropriate security. In other cases, 90.9 percent of viruses, worms, spyware and logic bomb cases, 87.5 percent of miscellaneous cases (including embezzlement and corruption), 82.6 percent of attack and sabotage cases, 80 percent of fraud cases, and 74.6 percent of hacking and illegal access cases are due to weak security.

Approximately 20 percent of fraud cases, approximately 16.9 percent of hacking and illegal access, and approximately 9.1 percent of viruses, worms, spyware and logic bomb could be classified into the category of medium security.

Only 17.4 percent of attack and sabotage, approximately 12.5 percent of miscellaneous (including embezzlement and corruption), and approximately 8.5 percent of hacking and illegal access succeeded in penetrating a well-protected computer system.

4.8. Complexity of Cybercrime

All the cases of data theft and espionage seem uncomplicated to commit. Approximately 87.5 percent of miscellaneous cases (including embezzlement and corruption), 80 percent of fraud cases, 73.9 percent of attack and sabotage cases, 66.7 percent of ID theft cases, and 66.1 percent of hacking and illegal access cases involved no complicated techniques or techniques that could be available to the most common computer or network user at the time of committing such offences.

Approximately 27.3 percent of viruses, worms, spyware and logic bomb cases, 20 percent of fraud cases, 12.3 percent of hacking and illegal access cases, and 8.7 percent of attack and sabotage cases are committed with moderately sophisticated techniques.

Cases of viruses, worms, spyware and logic bombs might involve the most complicated techniques, 72.7 percent of which fell into the most complicated category. Approximately 33.3 percent of ID theft cases, 18.3 percent of hacking and illegal access cases, 17.4 percent of attack and sabotage cases, and 12.5 percent of miscellaneous cases might involve complicated techniques or techniques unavailable to common users at the time of committing such offences.

4.9. Imprisonment Sentences

The punishments for many cases are labelled as "to be decided." This study calculated the punishment of the sentenced cases**.** The average imprisonment sentence for the data theft and espionage cases is 50 months, which is the longest among all the categories of cybercrimes. Cases of virus, worms, spyware, and logic bomb; and miscellaneous offences have the same average imprisonment sentence of 40.3 months. Fraudsters received an average imprisonment sentence of 32.5 months. Attack and sabotage cases are sentenced to an average imprisonment term of 28.1 months. The shortest average imprisonment term, 21.9 months, is imposed on hacking and illegal access perpetrators, namely the hackers.

The total imprisonment term imposed on the reported 53 offenders is 1429 months, with an average of shorter than 27 months. Among these cases, the longest imprisonment is 96 months, while the shortest is only one month.

4.10. Fine Sentences

A fine is typically imposed on perpetrators of hacking and illegal access, and attack and sabotage cases. Overall, exactly ten cases ended with a fine of less than USA$10,000, nineteen cases with a fine between USA$10,000 and USA$100,000, twelve cases with a fine between USA$100,000 and USA$1 million, and two cases with a fine over USA$1 million (one case was fined USA$2 million and the other case was fined USA$7.8 million).

The fine imposed on 43 offenders totalled USA$13.45 million, with an

average of USA$312,780. However, this sum is largely due to the heavy fines in two cases where the offenders were fined USA$2 million and USA$7.8 million, which contributed to an excess of USA$228,000 for the calculation of average fine. If these two cases are excluded from calculations, the average fine is approximately USA$89,000.

*

5. DISCUSSION AND CONCLUSION

THE SUBJECTS OF CYBERCRIMES CAN BE either insiders or outsiders. Many studies have found that insiders constitute a great threat to employers' systems. However, younger juveniles are less likely to be employed and may represent the increasing number of outsiders engaged in cybercrimes. On the other hand, the nature of cybercrime is such that there is no age limit. Anyone who can use computers and the internet can commit a cybercrime.

In my opinion, the concept of white-collar crime cannot fit the situation of cybercrime. Although white-collar crime emphasizes the employment and social status of the criminals, I consider that one of the most relevant factors in white-collar crime is the knowledge criminals have acquired from both their pre-employment education and their occupational career. It is not oversimplified to view white-collar crime as a knowledge-based offence, compared with violence-based traditional offences. As opposed to these two conceptions, cybercrime could be either knowledge-based white-collar crime or knowledge-based cyber violence. Overall, there is a reluctant distinction between cybercrime, white-collar crime and even violent crime.

However, it is reasonable to conclude that when there were few computers, employees in the computer-related industries were among the small number of computer users. They had more chances to commit an offence against their employers. With the prevalence of personal computers and the development of the internet, insiders maintain the advantage of having better knowledge about access control mechanisms, assets management systems, and overall loopholes. Insider knowledge, convenience, and directness encourage employees to commit cybercrimes. As the United States Secret Service and CERT Coordinator Center's study disclosed, minimal technical skill was required to launch cyberattacks on the banking and finance sector.[34]

In addition, insiders are exposed to the negative psychological influence derived from their information work environment. Shaw, Ruby and Post identified characteristics that increase the tendency towards illegitimate and harmful behaviour of the employees: "computer dependency, a history of personal and social frustrations (especially anger toward authority), ethical flexibility, a mixed sense of loyalty, entitlement, and a lack of empathy."[35]

On the other hand, the offences by insiders involve a less complicated

34. Marisa Reddy Randazzo, Michelle Keeney, Eileen Kowalski, Dawn Cappelli, and Andrew Moore, "Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector," Technical Report, CMU/SEI-2004-TR-021 (Carnegie Mellon Software Engineering Institute, 2005), <http://www.sei.cmu.edu/pub/documents/04.reports/pdf/04tr021.pdf> at pp. 9, 23. Insider was defined as "current or former employees or contractors." *ibid* at p. 5.
35. Shaw, Ruby, and Post, "The Insider Threat" *supra* note 23 at "Personal and Cultural Vulnerabilities."

process of being traced, detected and investigated than those by outsiders. If we could not judge whether insiders or outsiders are liable for more cybercrimes, we should firstly consider the question of who is more likely to commit cybercrimes and who is more likely to be caught. The insiders are both more likely to offend and more likely to get caught than outsiders. Furthermore, it is more efficient for law enforcement to uncover an inside than an outside attack. They are rationally more likely to pay more attention to the current and previous employees. The outside incidents or international disturbances would possibly be disregarded at the first sight of the investigation, unless it arouses broad concern in international society.

In summary, the study found that males are responsible for a majority of cybercrime. The cybercriminals are primarily between the ages of 17 to 45 years old. Domestic perpetrators constitute the absolute majority of the cybercriminals. Outsiders are four times more likely to be involved in cybercrimes than insiders. A large part of cybercrimes did not cause economic loss. However, once economic losses were involved, the average sum could reach as high as USA$1 million. The most vulnerable interests are in the private sector, even though threats to the public sector have usually been given more attention. The security levels of the victims are surprisingly weak, vulnerable to unsophisticated cybercrimes. Penalties against cybercrime, whether imprisonment or fines, are generally light.

The limit of this study is that the sample cases are randomly selected and published on the United States of America Department of Justice website. They could be regarded as typical cybercrime cases, but it is difficult to say whether they could be considered representative of cybercrimes happening in the United States. Therefore, this study is an explanation of the cases as examined. The sample survey method is usually used to give a sketch of the whole through the part, but this study warns against generalization of its findings to all cybercrimes. To avoid the shortcomings in the methods, the ideal study should cover a random sample in a wider range of cases, if it is available.

Appendix: Table of Statistical Data

115 cases 151 persons 1 company		Hacking, illegal access		Attack, sabotage, botnet		Virus, worms, spyware, logic bomb		Data theft, espionage		ID theft		Fraud		Other: embezzling, corruption	
		No.	%	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Gender	**Male**	61	96.8	23	100	11	100	7	100	26	100	7	100	13	92.9
	Female	2	3.2	0	0	0	0	0	0	0	0	0	0	1	7.1
	Total	63	100	23	100	11	100	7	100	26	100	7	100	14	100
Age	**-16**	2	3.2	0	0	1	0	0	0	0	0	0	0	0	0
	17-25	20	31.7	7	30.4	2	18.2	0	0	5	19.2	3	42.9	4	28.6
	26-35	18	28.6	6	26.1	2	18.2	3	42.9	1	3.8	2	28.6	7	50
	36-45	12	19	2	8.7	3	27.3	1	14.3	0	0	2	28.6	1	7.1
	46-	1	1.6	1	4	1	9.1	2	28.6	1	3.8	0	0	0	0
	N/A	10	15.9	7	30.4	2	18.2	1	14.3	19	73.1	0	0	2	14.3
Perpetrator	**Insider**	15	23.8	3	13	2	18.2	7	100	0	0	4	57.1	1	7.1
	Outsider	48	76.2	20	87	9	81.8	0	0	26	100	3	42.9	13	92.9
	Former employee	Inclu. 8	12.7	Inclu. 10	43.5	0	0	0	0	0	0	0	0	1	7.2
Loss	**No**	33	N/A	12	N/A	7	N/A	5	N/A	1	N/A	4	N/A	6	N/A
	-10k	4(21k)	N/A	2(10k)	N/A	1(5k)	N/A	1(5k)	N/A	0	N/A	0	N/A	0	N/A
	10k-100k	15(753k)	N/A	3(69k)	N/A	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A
	100k-1m	4(1076k)	N/A	6(1.679M)	N/A	0	N/A	0	N/A	0	N/A	1(384k)	N/A	1(875k)	N/A
	1m-	5(34.3M)	N/A	0	N/A	3(93M)	N/A	0	N/A	2(8M)	N/A	0	N/A	1(6.3M)	N/A
	Total	28(36.15M)	N/A	11(1.758M)	N/A	4(93.005M)	N/A	1(5k)	N/A	2(8M)	N/A	1(384k)	N/A	2(7.175k)	N/A

115 cases
151 persons
1 company

		Hacking, illegal access		Attack, sabotage, botnet		Virus, worms, spyware, logic bomb		Data theft, espionage		ID theft		Fraud		Other: embezzling, corruption	
		No.	%	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Citizenship	**Foreigner**	1 case	N/A	1 case	N/A	0	N/A	0	N/A	1 case	N/A	1 case	N/A	1 case	N/A
Imprisonment	**1-6**	5(24)	N/A	2(11)	N/A	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A
	7-12	9(101)	N/A	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A
	13-24	7(136)	N/A	4(81)	N/A	2(80)	N/A	1(18)	N/A	0	N/A	0	N/A	0	N/A
	25-36	7(224)	N/A	2(72)	N/A	0	N/A	1(36)	N/A	0	N/A	2(65)	N/A	2(70)	N/A
	>37	4(217)	N/A	2(117)	N/A	1(41)	N/A	1(96)	N/A	0	N/A	0	N/A	1(51)	N/A
	TBD	27	N/A	13	N/A	5	N/A	3	N/A	3	N/A	3	N/A	5	N/A
Fine	**<10k**	7(31.6k)	N/A	1(5k)	N/A	1(5k)	N/A	0	N/A	0	N/A	0	N/A	1(5k)	N/A
	10-100k	13(512.6k)	N/A	5(187.8k)	N/A	1(17k)	N/A	0	N/A	0	N/A	0	N/A	0	N/A
	100k-1m	5(1.368M)	N/A	4(643.8k)	N/A	0	N/A	0	N/A	0	N/A	2(624k)	N/A	1(250k)	N/A
	>1m	0	N/A	0	N/A	1(2m)	N/A	0	N/A	0	N/A	0	N/A	1(7.8M)	N/A
	TBD	32	N/A	13	N/A	7	N/A	6	N/A	3	N/A	3	N/A	5	N/A
Nature of victim	**Public**	8	13.6	4	18.2	0	0	0	0	0	0	0	0	1	12.5
	Private	41	69.5	17	77.3	9	81.8	5	100	3	100	4	100	7	87.5
	Private, public	9	15.3	0	0	1	9.1	0	0	0	0	0	0	0	0
	Public health and safety	1	1.7	1	4.5	1	9.1	0	0	0	0	0	0	0	0

115 cases
151 persons
1 company

		Hacking, illegal access		Attack, sabotage, botnet		Virus, worms, spyware, logic bomb		Data theft, espionage		ID theft		Fraud		Other: embezzling, corruption	
		No.	%	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Security levels of victims	**Strong**	5	8.5	4	17.4	0	0	0	0	0	0	0	0	1	12.5
	Medium	10	16.9	0	0	1	9.1	0	0	0	0	1	20	0	0
	Weak	44	74.6	19	82.6	10	90.9	6	100	3	100	4	80	7	87.5
Technique availability to others	**Complicated**	11	18.6	4	17.4	8	72.7	0	0	1	33.3	0	0	1	12.5
	Medium	9	12.3	2	8.7	3	27.3	0	0	0	0	1	20	0	0
	Simple	39	66.1	17	73.9	0	0	6	100	2	66.7	4	80	7	87.5