Computer Crimes Encountered among the Selected Companies in Metro Manila, Philippines

Review of
Integrative
Business &
Economics
Research

Harvey T. Ong
Decision Sciences and Innovation Department
Ramon V. del Rosario College of Business
Email : Harvey.Ong@dlsu.edu.ph, Harvs_Ong@yahoo.com

ABSTRACT

One major ethical issues related to IT and IS is property and accessibility to information. There are numerous threats to information security, which includes internet attacks, management failures, natural disasters, deliberate acts, man-made disasters, technical failures and unintentional acts.

The objective of the study is to identify and describe the threats to Information System and computer crimes encountered by the selected top corporations in Metro Manila, Philippines. This study can help companies avoid legal problems, and practice intellectual property which is the intangible property created by individuals or corporations that are protected under trade secret, patent and copyright laws. The research design used was descriptive. The data gathered (survey and interview results) from the respondent companies will be used for analysis.

Based on the data gathered (survey and interview results) from the 58 respondent companies which was used to discuss the threat to IS and computer crimes that had been encountered by them, the proponent found out that most common intellectual property related to IS usually deals with software, like copyright violation is a major problem for software vendors. Based on the findings, 27 out of 58 companies (or 46.55 %) mentioned that their computer crime experience was unauthorized access to computer files. 25 out of 58 respondents (or 43.10%) mentioned data communications fraud. 19 out of 58 respondents (or 32.76 %) mentioned about unlawful copying of copyrighted software. 18 companies (or 31.03%) mentioned credit card fraud, and 2 out of 58 companies (or 3.45%) mentioned others.

Keywords: Computer crime, threat to IS, legal issues, ethical issues

I. INTRODUCTION

1.1 Background of the Study

Copyright © 2012 Society of Interdisciplinary Business Research (www.sibresearch.org)

Computer crime, or **cybercrime**, refers to any crime that involves a computer and a network (Moore, 2005). The computer may have been used in the commission of a crime, or it may be the target (Kruse and Heiser, 2002). **Netcrime** refers to criminal exploitation of the Internet. Such crimes may threaten a nation's security and financial health (Mann and Sutton, 2011). Issues surrounding this type of crime have become high-profile, particularly those surrounding cracking, copyright infringement, child pornography, and child grooming (ISS, 2005). There are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise. Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Activity crossing international borders and involving the interests of at least one nationstate is sometimes referred to as cyber warfare. The international legal system is attempting to hold actors accountable for their actions through the International Criminal Court (Luke.duke.edu, 2011).

The word "hacker" originally referred to an enthusiastic, self taught computer user, but now the term usually describes a person who gains access to computer systems illegally. Computer criminals are likely to be trusted employees with no previous law-breaking experience. Many are motivated by resentment toward an employer, by personal or family problems, by the challenge of beating the system, or by tempting ease with which the crime can be committed. There are three basic types of computer crime : (1) theft of computer time for development of software (2) theft, destruction, or manipulation of programs and data, and (3) alteration of data stored in a computer file. (Capron and Johnson, 2004).

Prosecution of computer crime is often difficult because some law enforcement officers, attorneys and judges are unfamiliar with the computer crime issues involved. However, starting 1986, there's a Computer Fraud and Abuse Act, it has improved awareness of computer related crimes, and most countries have passed some of computer crime law.

1.2 Rationale of the Study

The proponent's interest on the topic of Information Systems Ethics, Privacy and Security began when the proponent started taking up the PhD in Business - Education subject under Atty. Jocelyn Cruz and when the proponent also embarked on teaching COMP1BU and COMP2BU (Computer Application for Business Management Students), ENTEMIS (Management Information System for Entrepreneurship), SYSTAND (System Analysis and Design), IS Planning and BUSIMIS (Management Information System for Business Management Students) for undergraduate of the Decision Sciences and Innovation Department – De La Salle University - Manila. And besides, the undergraduate degree of proponent was Computer Science specialized in Software Technology. Lastly, the proponent has the interest to look into the information system threats and computer crimes encountered by different companies, it is worth knowing because we all should aware the problem of computer crime, criminal profiles, crime types, the need for security including disaster recovery plan, software and data security, and security legislation. In addition, as a good citizenship of the country, we should understand the importance of ethics as related to a computer environment, and the proper

Copyright © 2012 Society of Interdisciplinary Business Research (www.sibresearch.org)

uses of Information System without any threats in security constantly helped companies to improve the way they conduct business transaction and make sure that it continues to meet their company's goals and objectives, and to cut costs and increase profits.

1.3 Statement of the Problem

What are the threats to Information System and Computer Crimes encountered by the selected top corporations in Metro Manila, Philippines ?

1.4 Objectives of the Study

The objective of the study is to identify and describe the threats to Information System and computer crimes encountered by the selected top corporations in Metro Manila, Philippines.

1.5 Significance of the Study

The result of the study will benefits the following :

- Faculty of Decision Sciences and Innovation Department and Computer Science – De La Salle University Manila

This will give the faculty teaching COMP1BU, COMP2BU, ENTEMIS, BUSIMIS, SYSTAND and INNOTEC an idea on what specific topic needs to include or discuss in class lecture, so the students would become aware of the problem of computer crime, including criminal profiles, types of crimes, and the difficulties of discovery and prosecution.

- Different corporations in Metro Manila, Philippines

To give them feedback on how different companies in Metro Manila encountered different threats to IS and computer crimes, this would let them become aware of the need for security, including disaster recovery plans, software and data security, and security legislation. The companies should also understand the importance of ethics as related to a computer environment.

1.6 Scope and Limitation

The company respondents focused on this study will be limited to 58 top corporations in Metro Manila, Philippines.

The data gathering was assisted by proponent' students in Entrepreneurship Information System class (1st term AY 2010-2011), and it was limited to 100 top corporations based on their gross revenue in Metro Manila, Philippines which was stated in Business World Magazines published early 2010. Business World Top 1000 Corporations in the Philippines is published annually by Business World Publishing Corporation, with editorial offices at 95 Balete Drive Extension, New Manila, Quezon City, Metro Manila, Philippines.

At first, the limitation of the study was limited to top 100 corporations based on their gross revenue which was stated in Business World magazines, but unfortunately, not all the 100 corporations responded. Some of them are not willing to be surveyed nor interviewed. Out of 100, only 58 corporations responded. In addition, only these 58 companies were accessible and located in Metro Manila. And these are composed of 22 service companies, 10 manufacturing companies and 26 merchandising companies.

The respondent also had a hard time to assess the data gathered from the companies. The data gathered was presented in narrative explanation format, this give the proponent a hard time in coding the data. Another limitation of the study was that there are some computer crimes encountered and other important details and information were not mentioned or discussed clearly by the interviewee respondent of the corporation. And many companies also claimed that these information are kept highly confidential by their companies.

II. REVIEW OF RELATED LITERATURE

According to Rainer and Turban (2009), “Protecting intellectual property is a vital issue for people who make their livelihood in knowledge fields. **Intellectual Property** is the property created by individuals or corporations that is protected under trade secrets, patent and copyright laws. A **trade secret** is an intellectual work, such as a business plan, that is company secret, and is not based on public information. An example is a corporate strategic plan. A patent is a document that grants the holder exclusive rights on an invention or process for 20 years. **Copyright** is a statutory grant that provides the creators of intellectual property with ownership of the property for the life of creator plus 70 years. Owners are entitled to collect fees from anyone who wants to copy the property. The U.S. Federal Computer Software Copyright Act (1980) provides protection for source and object code of computer software, but the law does not clearly identify what is eligible for protection. For example, copyright law does not protect similar concepts, functions, and general features such as pull-down menus, colors, and icons. However, copying a software program without making payment to the owner – including giving a disc to a friend to install on his or her computer – is a copyright violation. Not surprisingly, this practice, called **piracy**, is a major problem for software vendors. The global trade in pirated software amounts to hundred billions of dollars. The Business Software Alliance (BSA), an organization representing the world’s commercial software industry, promoted legal software and conducts research on software piracy in an attempt to eliminate it. The BSA (www.bsa.org) has identified Vietnam, China, Indonesia, Ukraine and Russia as the countries with the high percentages of illegal software. More than 85 percent of the software used in these countries consists of illegal copies.

According to http://en.wikipedia.org/wiki/Computer_crime website, it states that : “Computer crime encompasses a broad range of activities. Generally, however, it may be divided into two categories: (1) crimes that target computers directly; (2) crimes facilitated by computer networks or devices, the primary target of which is independent of the computer network or device.

Crimes that primarily target computer networks or devices include:

- Computer viruses
- Denial-of-service attacks
- Malware (malicious code)

Crimes that use computer networks or devices to advance other ends include:

- Cyberstalking
- Fraud and identity theft
- Information warfare
- Phishing scams

Spam

Spam, or the unsolicited sending of bulk email for commercial purposes, is unlawful in some jurisdictions. While anti-spam laws are relatively new, limits on unsolicited electronic communications have existed for some time.

Fraud

Computer fraud is any dishonest misrepresentation of fact intended to let another to do or refrain from doing something which causes loss. In this context, the fraud will result in obtaining a benefit by:

- Altering computer input in an unauthorized way. This requires little technical expertise and is not an uncommon form of theft by employees altering the data before entry or entering false data, or by entering unauthorized instructions or using unauthorized processes;
- Altering, destroying, suppressing, or stealing output, usually to conceal unauthorized transactions: this is difficult to detect;
- Altering or deleting stored data;
- Altering or misusing existing system tools or software packages, or altering or writing code for fraudulent purposes.

Other forms of fraud may be facilitated using computer systems, including bank fraud, identity theft, extortion, and theft of classified information.

Copyright © 2012 Society of Interdisciplinary Business Research (www.sibresearch.org)

A variety of Internet scams target consumers direct.

Obscene or offensive content

The content of websites and other electronic communications may be distasteful, obscene or offensive for a variety of reasons. In some instances these communications may be illegal.

Over 25 jurisdictions place limits on certain speech and ban racist, blasphemous, politically subversive, libelous or slanderous, seditious, or inflammatory material that tends to incite hate crimes.

The extent to which these communications are unlawful varies greatly between countries, and even within nations. It is a sensitive area in which the courts can become involved in arbitrating between groups with strong beliefs.

One area of Internet pornography that has been the target of the strongest efforts at curtailment is child pornography.

Harassment

Whereas content may be offensive in a non-specific way, harassment directs obscenities and derogatory comments at specific individuals focusing for example on gender, race, religion, nationality, sexual orientation. This often occurs in chat rooms, through newsgroups, and by sending hate e-mail to interested parties (see cyber bullying, cyber stalking, harassment by computer, hate crime, Online predator, and stalking). Any comment that may be found derogatory or offensive is considered harassment.

Drug trafficking

Drug traffickers are increasingly taking advantage of the Internet to sell their illegal substances through encrypted e-mail and other Internet Technology.Some drug traffickers arrange deals at internet cafes, use courier Web sites to track illegal packages of pills, and swap recipes for amphetamines in restricted-access chat rooms.

The rise in Internet drug trades could also be attributed to the lack of face-to-face communication. These virtual exchanges allow more intimidated individuals to more comfortably purchase illegal drugs. The sketchy effects that are often associated with drug trades are severely minimized and the filtering process that comes with physical interaction fades away.

Cyber terrorism

Government officials and Information Technology security specialists have documented a significant increase in Internet problems and server scans since early 2001. But there is a growing concern among federal officials[*who?*] that such intrusions are part of an organized effort by cyberterrorists, foreign intelligence services, or other groups to map potential security holes in critical systems. A cyberterrorist is someone who intimidates or coerces a government or organization to advance his or her political or social

Copyright © 2012 Society of Interdisciplinary Business Research (www.sibresearch.org)

objectives by launching computer-based attack against computers, network, and the information stored on them.

Cyber terrorism in general, can be defined as an act of terrorism committed through the use of cyberspace or computer resources (Parker 1983). As such, a simple propaganda in the Internet, that there will be bomb attacks during the holidays can be considered cyberterrorism. As well there are also hacking activities directed towards individuals, families, organized by groups within networks, tending to cause fear among people, demonstrate power, collecting information relevant for ruining peoples' lives, robberies, blackmailing etc.

Cyberextortion is a form of cyberterrorism in which a website, e-mail server, or computer system is subjected to repeated denial of service or other attacks by malicious hackers, who demand money in return for promising to stop the attacks. According to the Federal Bureau of Investigation, cyberextortionists are increasingly attacking corporate websites and networks, crippling their ability to operate and demanding payments to restore their service. More than 20 cases are reported each month to the FBI and many go unreported in order to keep the victim's name out of the domain. Perpetrators typically use a distributed denial-of-service attack.

Cyber warfare

Sailors analyze, detect and defensively respond to unauthorized activity within U.S. Navy information systems and computer networks

The U.S. Department of Defense (DoD) notes that cyberspace has emerged as a national-level concern through several recent events of geo-strategic significance. Among those are included the attack on Estonia's infrastructure in 2007, allegedly by Russian hackers. "In August 2008, Russia again allegedly conducted cyber attacks, this time in a coordinated and synchronized kinetic and non-kinetic campaign against the country of Georgia. Fearing that such attacks may become the norm in future warfare among nation-states, the concept of cyberspace operations impacts and will be adapted by warfighting military commanders in the future.

Documented cases

One of the highest profiled banking computer crime occurred during a course of three years beginning in 1970. The chief teller at the Park Avenue branch of New York's Union Dime Savings Bank embezzled over $1.5 million from hundreds of accounts.

A hacking group called the MOD (Masters of Deception), allegedly stole passwords and technical data from Pacific Bell, Nynex, and other telephone companies as well as several big credit agencies and two major universities. The damage caused was extensive, one company, Southwestern Bell suffered losses of $370,000 alone.

In 1983, a nineteen year old UCLA student used his PC to break into a Defense Department international communications system.

Between 1995 and 1998 the Newscorp satellite pay to view encrypted SKY-TV service was hacked several times during an on-going technological arms race between a pan-European hacking group and Newscorp. The original motivation of the hackers was to watch Star Trek re-runs in Germany; which was something which Newscorp did not have the copyright to allow.

On 26 March 1999, the Melissa worm infected a document on a victim's computer, then automatically sent that document and copy of the virus via e-mail to other people.

In February 2000 a individual going by the alias of MafiaBoy began a series denial-of-service attacks against high profile websites, including Yahoo!, Amazon.com, Dell, Inc., E*TRADE, eBay, and CNN. About fifty computers at Stanford University, and also computers at the University of California at Santa Barbara, were amongst the zombie computers sending pings in DDoS attacks. On 3 August 2000, Canadian federal prosecutors charged MafiaBoy with 54 counts of illegal access to computers, plus a total of ten counts of mischief to data for his attacks.

The Russian Business Network (RBN) was registered as an internet site in 2006. Initially, much of its activity was legitimate. But apparently the founders soon discovered that it was more profitable to host illegitimate activities and started hiring its services to criminals. The RBN has been described by VeriSign as "the baddest of the bad".[11] It offers web hosting services and internet access to all kinds of criminal and objectionable activities, with an individual activities earning up to $150 million in one year. It specialized in and in some cases monopolized personal identity theft for resale. It is the originator of MPack and an alleged operator of the Storm botnet.

On 2 March 2010, Spanish investigators busted 3 in infection of over 13 million computers around the world. The "botnet" of infected computers included PCs inside more than half of the Fortune 1000 companies and more than 40 major banks, according to investigators.

In August 2010 the international investigation Operation Delego, operating under the aegis of the Department of Homeland Security, shut down the international pedophile ring Dreamboard. The website had approximately 600 members, and may have distributed up to 123 terabytes of child pornography (roughly equivalent to 16,000 DVDs). To date this is the single largest U.S. prosecution of an international child pornography ring; 52 arrests were made worldwide.

Combatting Computer Crime

A computer can be a source of evidence. Even when a computer is not directly used for criminal purposes, may contain records of value to criminal investigators. " (http://en.wikipedia.org/wiki/Computer_crime, 2011)

According to http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act, it states that "Computer Fraud and Abuse Act is a law passed by the United States Congress in 1986, intended to reduce cracking of computer systems and to address federal computer-related offenses. The Act (codified as 18 U.S.C. § 1030) governs cases with a compelling federal interest, where computers of the federal government or certain financial institutions are involved, where the crime itself is interstate in nature, or where computers are used in interstate and foreign commerce. It was amended in 1988, 1994, 1996, in 2001 by the USA PATRIOT Act, 2002, and in 2008 by the Identity Theft Enforcement and Restitution Act. Subsection (b) of the act punishes anyone who not just commits or attempts to commit an offense under the Act, but also those who conspire to do so.

1. Knowingly accessing a computer without authorization in order to obtain national security data

2. Intentionally accessing a computer without authorization to obtain:

   - Information contained in a financial record of a financial institution, or contained in a file of a consumer reporting agency on a consumer.

   - Information from any department or agency of the United States

   - Information from any protected computer if the conduct involves an interstate or foreign communication

3. Intentionally accessing without authorization a government computer and affecting the use of the government's operation of the computer.

4. Knowingly accessing a protected computer with the intent to defraud and there by obtaining anything of value.

5. Knowingly causing the transmission of a program, information, code, or command that causes damage or intentionally accessing a computer without authorization, and as a result of such conduct, causes damage that results in:

   - Loss to one or more persons during any one-year period aggregating at least $5,000 in value.

   - The modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of one or more individuals.

   - Physical injury to any person.

   - A threat to public health or safety.

   - Damage affecting a government computer system

6. Knowingly and with the intent to defraud, trafficking in a password or similar information through which a computer may be accessed without authorization. “

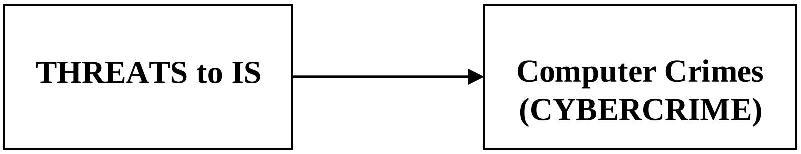
III. FRAMEWORK

3.1 Conceptual Framework

The conceptual framework of the study is based on (or adopted from) R. Kelly Rainer Jr. and Efraim Turban which states the following :

There are numerous threats to information security, which fall into the general categories of unintentional and intentional. Unintentional threats include human errors, environmental hazards, and computer system failures. Intentional failures includes espionage, extortion, vandalism, theft, software attacks, and compromises to intellectual property. A growing threat is computer crime or cybercrime, which often utilizes identify theft and phishing attacks. (please see figure 1):

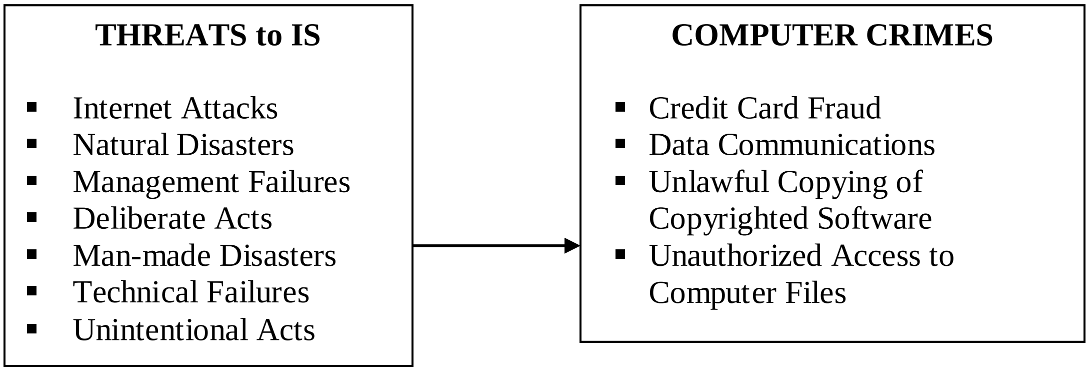
Figure 1 : Schematic Diagram of the Conceptual Framework



3.2 Operational Framework

Adopted from the Conceptual Framework of Reynolds and Stairs (2009), the threats to the information system encountered by selected top corporations in Metro Manila and its computer crimes will serve as the variables of this study in terms of :

Figure 2 : Variables of the study



3.3 Operational Definition of Terms

Copyright © 2012 Society of Interdisciplinary Business Research (www.sibresearch.org)

- *Computer Crimes – refers to Credit Card Fraud, Data Communications, Unlawful Copying of Copyrighted Software and Unauthorized Access to Computer Files*
- *Credit Card Fraud – refers to customer credit card numbers that are used fraudulently*
- *Data Communications – refers to piggybacking on some else's network the use of an office for personal purposed and computer directed diversion of funds*
- *Deliberate Acts – refers to unauthorized copying and theft of sensitive information.*
- *Internet Attacks – refers to virus and hackers*
- *Management Failures – refers to lack of funding, interest for information security effort*
- *Man-made Disasters – refers to fire, power outage, and etc.*
- *Natural Disasters – refers to floods and earthquakes*
- *Technical Failures – refers to hard drive crash*
- *Threats to IS – refers to Internet Attacks, Natural Disasters, Management Failures, Deliberate Acts, Man-made Disasters, Technical Failures and Unintentional Acts.*
- *Unintentional Acts – refers to opening questionable emails, careless internet surfing, poor password selection, unlocked filing cabinets, not logging off the company network.*
- *Unauthorized Access to Computer Files – refers to accessing confidential employees records, theft of trade secrets and product pricing structures*
- *Unlawful Copying of Copyrighted Software – refers to sharing of copyrighted software or assembly-line copying*

IV. RESEARCH METHODOLOGY

4.1 Research Design

The research design used was descriptive. The data gathered (survey and interview results) from the respondent companies will used to identify and describe the conversion strategies adopted by the selected top corporations in Metro Manila, Philippines. The study will also look into the perceived advantages considered by the 58 corporations in Metro Manila.

Among the 100 list of corporations, only 58 companies responded. 22 companies (or 37.93 %) were Service companies which includes oil refineries, electric distribution, wireless service, banking, power service, port management, media, financial institution, utility, real estate, telecommunications, transportation, infrastructure, water, call center, and insurance companies. 10 companies (or 17.24 %) responded were Manufacturing companies which includes food, automotive, agriculture, beverage and beers, pharmaceutical, pediatric nutrition, cement, packaging companies. And 26 companies (or 44.83%) were Merchandising companies which includes shopping and retail, supermarket, warehousing, beauty products, LPG and Petroleum companies.

Copyright © 2012 Society of Interdisciplinary Business Research (www.sibresearch.org)

4.2 Sampling Plan

The secondary data collected during 1st term Academic Year 2010-2011 from the corporation interviewed by ENTEMIS students as the basis of data for this research study.

4.3 Method of Data Analysis

Primary data was tabulated in a data set, and the data was analyzed using the frequency and percentage distribution. Since the data gathered presented in narrative paragraph form, content analysis will be used by the proponent in coding the data. And the data was presented also in frequency distribution table format and context narrative discussion.

V. RESEARCH FINDINGS

<u>Based from the Conceptual Framework adapted by the proponents :</u>

The purpose of using the conceptual framework stated in the previous section is to identify and describe the threats to IS and computer crimes adopted by the selected top corporations in Metro Manila, Philippines. This would also describe the social context and corporate culture of the companies studied – the values and beliefs that determine what is admissible and possible within the culture of their corporations involved.

THREATS TO IS ENCOUNTERED BY THE TOP CORPORATIONS

Table 1 : Frequency and percentage distribution results with regards to threats to IS

	Frequency (n = 58)	%
▪ Internet Attacks	53	91.38 %
▪ Natural Disasters	34	58.62 %
▪ Management Failures	42	72.41 %
▪ Deliberate Acts	53	91.38 %
▪ Man-made Disasters	24	41.38 %
▪ Technical Failures	28	48.28 %
▪ Unintentional Acts	33	56.90 %

In table 1, it shows that 53 out of 58 companies (or 91.38 %) mentioned that their threats to IS were internet attacks and deliberate acts. These companies states that these usually caused by their own employees (or insiders) account for a large

Copyright © 2012 Society of Interdisciplinary Business Research (www.sibresearch.org)

number of information security breaches, for example, trespass of access, information extortion, theft of equipment or information, identity theft, compromises to intellectual property, software attacks, cyberterrorism and cyberwarfare, and etc.

Next highest, 42 out of 58 companies (or 72.41 %) mentioned that management failures was their threat to IS. They stated that these involve a lack of funding for information security efforts and sometimes negligence or lack of interest in those efforts. This cause the information security of the organization to suffer and lead to computer crimes.

Rank number three, 34 out of 58 respondents (or 58.62 %) mentioned about natural disasters. The companies mentioned the natural calamities include floods (caused by Ondoy and Pedring typhoons), earthquake, lightning, and, in some cases, fires. Companies mentioned that there are many cases which was caused by acts of God which they losses their systems and data.

On the other hand, 33 out of 58 respondents (or 56.90 %) mentioned that their threat to IS was actually unintentional acts only. The companies states that these with mo malicious intent, for example human errors, deviations in the quality of services by ISP (Internet Service Provider) and hazards caused by environment.

28 out of 58 companies (or 48.28 %) said technical failures was their major problem. They mentioned that they encountered problems with hardware, software, and networking. Their most common problem was crash of a hard disk drive which they don’t have any back up. In some cases, software problems which contain bugs are also common to them.

And only 24 out of 58 companies (or 41.38 %) mentioned man-made disasters.

COMPUTER CRIMES ENCOUNTERED BY THE TOP CORPORATIONS

Table 2 : Frequency and percentage distribution results with regards to Computer Crimes encountered by the companies

	Frequency (n = 58)	%
Credit Card Fraud	18	31.03 %
Data Communications Fraud	25	43.10 %
Unlawful Copying of Copyrighted Software	19	32.76 %
Unauthorized Access to Computer Files	27	46.55 %
Others	2	3.45 %

In table 2, it shows that 27 out of 58 respondents (or 46.55 %) mentioned that their experience in computer crime was unauthorized access to computer files. Many companies experienced that the hackers try to gain access to confidential

Copyright © 2012 Society of Interdisciplinary Business Research (www.sibresearch.org)

employee records, company trade secrets and product pricing structures, and much more.

Rank number 2, 25 out of 58 respondents (or 43.10%) mentioned that data communications fraud was their encountered computer crime. This form of fraud involves the interceptions of network passwords or packets of data passing through networks.

Next highest, 19 out of 58 respondents (or 32.76 %) mentioned about unlawful copying of copyrighted software. The companies also states that when they encountered this category of computer crime, it results in major losses for computer vendors. The most common intellectual property related to IS usually deals with software, to be more specific, copyright violation is a major problem for software vendors.

While 18 companies (or 31.03%) stated that credit card fraud was their crime in the workplace. They mentioned that credit card customer numbers pass between public and private networks, sometimes these numbers are captured by computer criminals and used to commit fraud.

And 2 out of 58 companies (or 3.45%) mentioned other forms of computer crime, and they didn’t specify what particular type of cybercrime.

V. CONCLUSION / OBSERVATION

The proponent embarked on this study in order to list down the computer crimes encountered by the companies in Metro Manila based on the surveyed and interviewed from 58 corporations, and to disseminate them in the academic and business community.

The data gathered (survey and interview results) from the respondent companies was used to discuss the threat to IS and computer crimes which were encountered by 58 companies in Metro Manila namely in the following sectors: Service, Manufacturing and Merchandising Corporations. Based on the surveyed and interviewed, the proponent found out that most common intellectual property related to IS among the top corporations in Metro Manila usually deals with software, to be specific, copyright violation is a major problem for software vendors. Based on the findings, 27 out of 58 companies (or 46.55 %) mentioned that their computer crime experience was unauthorized access to computer files. Rank number 2, 25 out of 58 respondents (or 43.10%) mentioned data communications fraud. Rank number 3, 19 out of 58 respondents (or 32.76 %) mentioned about unlawful copying of copyrighted software. Rank number 4, 18 companies (or 31.03%) mentioned credit card fraud, and 2 out of 58 companies (or 3.45%) mentioned others.

Based on proponent's observation, a system of safeguards is needed for the companies to protect their information system and data from deliberant or accidental damage or access by unauthorized persons. To assure this, it should only the right person is accessing the right information at the right computer system. Companies should also come up with a disaster recovery plan, they should spells out a method for restoring computer processing operation and data files, in addition, they should perform emergency recovery drills. Furthermore, the companies should consult a lawyer or they should aware of the following : Fair Credit Reporting Act, Freedom of Information Act, Federal Privacy Act, Video Piracy Protection Act, Computer Matching / Privacy Protection Act and others.

The proponent would like to quote the statement of Rainer and Turban (2009) for recommendation that : "Information systems are protected with a wide variety of controls such as security procedures, physical guards, and detection software. These can be classified as controls used for prevention, deterrence, detection, damage control, recovery, and correction of information systems. The major types of general controls include physical controls, access controls, administrative controls, and communication controls. Application controls include input, processing and output controls. Information systems auditing is done in a similar manner to accounting and financing auditing, around, through, and with the computer. A detailed internal and external IT audit may involve hundreds of issues and can be supported by both software and checklists. Related to IT auditing is the preparation for disaster recovery, which specifically addresses how to avoid, plan for, and quickly recover from a disaster." (Rainer and Turban, 2009)

There are some suggestions to avoid computer crimes in the workplace : (1) Avoid common names – common names associated with you are easy for you to remember, but they are easily cracked (2) Use mix and match characters in your password – make your password a mix of letters and numbers, upper and lower cases, alphabetic and numeric characters, (3) Store password wisely – keep you password in your head, keep it to yourself, or in a safe, not in an obvious locations, (4) Change your password often – change your password should become a habit so that you will lessen the chance of it becoming known to others, (5) Avoid hacker scam – in these scam, the hacker poses as a person to whom you can confide your password, wise user will not give their password to anyone or write their password in their own planner or wallet.

Lastly, ethical, security and privacy are important issues in Information Age. The IT industry as well as private citizens should share responsibility in addressing these issues in able to guide our country into more growth and prosperity.

VII. REFERENCES

[1] Capron and Johnson (2004) "Computers : Electronic Tools for an Information Age" 8th Edition, Paerson Prentice Hall

Copyright © 2012 Society of Interdisciplinary Business Research (www.sibresearch.org)

[2] "Cyber Warfare and the Crime of Aggression: The Need For Individual Accountability on Tomorrow's Battlefield" Law.duke.edu. David Mann and Mike Sutton (2011-11-06) Bjc.oxfordjournals.org

[3] Internet Security Systems. March-2005.

[4] Moore, R. (2005) "Cybercrime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.

[5] Rainer and Turban (2009) "Introduction to Information Systems : Enabling and Transforming Business" John wiley & Sons, Inc.

[6] Warren G. Kruse, Jay G. Heiser (2002). *Computer forensics: incident response essentials*. Addison-Wesley. p. 392. ISBN 0201707195.

[7] http://www.law.duke.edu/journals/dltr/articles/2010dltr003.html. Retrieved 2011 -11-10.

[8] http://bjc.oxfordjournals.org/cgi/content/abstract/38/2/201. Retrieved 2011-11-10.

[9] http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act

Copyright © 2012 Society of Interdisciplinary Business Research (www.sibresearch.org)