COMPUTER ABUSE, SOCIAL BOND FACTORS AND THE ROLE OF INFORMATION AND COMMUNICATION TECHNOLOGY DETERRENTS AS MODERATOR IN THE MALAYSIAN PUBLIC ORGANIZATIONS

AHMAD SUHAIMI BIN BAHARUDIN

UNIVERSITI SAINS MALAYSIA

2007

COMPUTER ABUSE, SOCIAL BOND FACTORS AND THE ROLE OF INFORMATION AND COMMUNICATION TECHNOLOGY DETERRENTS AS MODERATOR IN THE MALAYSIAN PUBLIC ORGANIZATIONS

by

AHMAD SUHAIMI BIN BAHARUDIN

Thesis submitted in fulfillment of the requirements
for the degree of
Doctor of Philosophy

September 2007

ACKNOWLEDGEMENT

Bismil-laahir-rahmaanir-rahim (In the name of Allah, Most Benevolent and Most Merciful). To my deceased father, Allahyarham Baharudin Bin Che Embi, I prayed that Allah the Al-Mighty will bless his kind soul as he was a loving and caring father who always encouraged me to seek higher education. To my mother Hajah Maznah Binti Haji Mahmud, my wife Puan Norhaida Binti Mohd Zamri, my lovely and bright 11 years old daughter Nur Atiqah Sorfina Binti Ahmad Suhaimi, my active and adventurous 10 years old son Ahmad Sufi Naim Bin Ahmad Suhaimi and my lovely and pampered eight years old daughter Nur Aliya Syahmin Binti Ahmad Suhaimi, I thank them for their patience, understanding, love, sacrifice and prayers that kept me going with my studies. To my two brothers and sister, Encik Ahmad Suhairi Bin Baharudin, Encik Ahmad Nazri Bin Baharudin and Puan Aida Suriati Binti Baharudin, I thank them for the motivation and concerned that they have given me.

My experience of undergoing a Ph.D. program in the Universiti Sains Malaysia (USM) is a long, most difficult and a very lonely journey. I am grateful that I am blessed with the two very well-experienced and dedicated supervisors Associate Professor Dr. Yuserrie Zainuddin and Associate Professor Ramayah Thurasamy who have guided me all the way through this difficult but most challenging journey. I have experienced many but yet unique obstacles at every stages of this research, should it be during the pre-proposal, proposal, data-collection, findings and post-findings stages. However, I have managed to overcome those obstacles successfully with their help. Each time after the weekly discussions with them, somehow both of them have created the atmosphere which made me felt very motivated and that is what kept pushing me back on the track right until the end of this course. To both of them, I wish to thank them for the wonderful advices, support and guidance, knowledge and confidence that both of them have given me in the course of preparing for my thesis. While I was under their supervisions, from my thesis, I have successfully published a paper in an international journal and have presented three papers in two local proceedings, and I thank to both of them for giving me the chance and such valuable exposures which I never had before I embarked into this program.

To Associate Professor Dr. Zainal Ariffin Ahmad, I wish to thank him for the constant support, advised and comments especially on the proper American Psychological Association (APA) formatting of my thesis. Special thanks to both Professor Dr. Mohamed Sulaiman and Dr. Noornina Dahlan, who have been providing me with fruitful and constructive comments and recommendations especially during my proposal and findings defenses. I would like to also convey my humble and sincere appreciation to the former Dean, School of Management, Yang Berbahagia Professor Dato' Dr. Daing Nasir Ibrahim, for his willingness to help and continuous support, concerned and encouragement that he has given me during my attachment with the School of Management.

In addition to that, I would like to also expressed my sincere thanks to all lecturers and staff of the school, for their wonderful support and motivation especially to Associate Professor Dr. Ishak Ismail (Dean), Associate Professor Dr. Zamri Ahmad (Deputy Dean), Professor Muhamad Jantan, Professor Osman Mohamad, Associate Professor Dr. Aizzat Haji Mohd Nasurdin, Associate Professor Dr. Fauziah Md. Taib, Associate Professor Datin Dr. Ruhani Haji Ali, Associate Professor Dr. Hasnah Haron, Dr. Suhaiza Hanim Mohamad Zailani, Datin Dr. Joriah Muhammad, Dr. Lilis Surienty Binti Abd Talib, Puan Aton @ Aminah Khaton Mohamad and Puan Rusnah Che Amat.

Also, I would like to extend my sincere gratitude to Dr. Sundramoorthy A/L M. Pathmanathan and Dr. Premalatha A/P Karupiah from the School of Social Sciences, for their wonderful ideas and comments on sociological theories, the Post Graduate Institute especially to Yang Berbahagia Datin Hajah Fazia Ali (Head Assistant Registrar), Hajah Jamaliah Sulaiman (Assistant Registrar) and Encik Amir Imran Zainoddin, for helping me with my registration and re-registration, to all staff of the Universiti Sains Malaysia Library especially to Encik Ariffin Bin Aziz, Encik Abd Basher Bin Abdullah, Encik Mohd Nasir Bin Abu Hashim, Encik Zainol Bin Abd Karim and Puan Habsah Abdul Rahman (Librarian) for helping me to get the needed materials for my research and to Pusat Terjemahan Dan Bahasa, USM especially to Puan Nor Aini Ali (Publication Officer), for helping me with the translation of my questionnaires. I am also grateful to all my colleagues in the Ph.D. program who have constantly encourages me to be patient and persevere, especially Dr. Hayati Mohd Dahan, Dr. Norjaya Binti Mohd Yasin, Assistant Professor Dr. Majdi Mohamad Medhat Al-Khalili, Dr. Mohamad Abdullah Hemdi, Dr. Herianto Puspowarsito, Dr. Jasman J. Ma’ruf, Dr. Abdel Hafiez A, Dr. Galumbang Hutagalung, Dr. Lena Ellitan, Dr. Kitima Tamalee, Bapak Iskandarsyah Madjid, Mr Joshua Ignatius, Dr. Haji Zahri Bin Hamat (from the School of Social Sciences, USM) and many more.

My gratitude also goes to the management of Penang Regional Development Authority (PERDA)/Prime Minister’s Department, especially to Encik Azmi Bin Lateh (General Manager of PERDA), Yang Berhormat Datuk Hilmi Bin Haji Abdul Rashid (Chairman of PERDA), Encik Saringat Bin Haji Hassan (Strategic Planning Section Manager), Hajah Noraishah Binti Che Dan (Administration and Finance Section Manager) and Cik Noor Hayati Binti Ishak (Assistant Manager), which approved my application for a full-paid leaves to pursue this Ph.D. Program and for allowing me to use the computer resources for my research.

I would like to also extend my sincere thanks to all staff of PERDA for the constant moral support and encouragement especially to Puan Hereti Binti Desa (Systems Analyst), Encik Roslan Bin Samsudin (Programmer), Puan Raudzoh Binti Haji Harun (Data Entry Clerk), Cik Noorasikin Binti Ismail (IT Technician), Encik Mohammad Zulkifli Ibrahim (Accountant), Encik Mohammad Fahimi Bin Abu Bakar (Internal Auditor), Encik Omar Bin Abdul Hamid (Legal Officer), Encik Rohaimi Bin Othman (Head of PERDA's Training Centre in Bukit Panchor, Nibong Tebal, Penang), Encik Abdul Aziz Bin Mohd Akhir (Assistant Manager), Encik Mohd Asri Bin Baharum (Assistant Manager) and many more.

My special thanks also goes to the Malaysian Public Service Department (Training Section), especially to Encik Razali Bin Ahmad, Puan Maziah Binti Adnan, Encik Tajuddin Don, Encik Mohd Bustaman Abdul Aziz, Encik Mohd Azman Bin Haji Mohd Ariffin, Encik Aszhary Bin Mohamad and Puan Halimahton Binti Suheimi, which provides me with the financial scholarship to pursue the Ph.D. program.

I would like to convey my greatest gratitude and appreciation to the past General Managers of PERDA especially to Yang Berbahagia Dato' Wan Ibrahim Bin Wan Daud, Tuan Haji Abd. Rahim Bin Saleh, Encik Tambi Abu Hassan and Yang Berbahagia Dato' Mohammad Izat Hasan for their concerned and support with my study. Also, special thanks to Yang Berbahagia Tan Sri Samsudin Bin Osman (the former Chief Secretary to the Government of Malaysia), Puan Rahmah Binti Ramli (the Special Officer to the Chief Secretary to the Government of Malaysia) and Yang Berbahagia Dato' Haji Othman Bin Desa (the Political Secretary to the Yang Amat Berhormat the Prime Minister of Malaysia).

I would like to convey my thanks to Mr. Norman Yeoh from Norman Office Supplies (Penang) for the printing of questionnaires and Encik Isahak Bin Osman from Sekolah Kebangsaan Permatang Tok Jaya, Seberang Perai Utara, Penang for his assistance in proof reading my thesis. My special thanks also to the family of Encik Kamarudin Bin Salleh, his wife, Puan Puzie Binti Kamal and his son, Encik Muhammad Miqdad Bin Kamarudin for helping me in the data entry process. I also would like to thank to the three young ladies from the Institute of Technology Tun Abdul Razak, Cik Aznem Binti Ahmad (Alor Setar), Cik Halinah Binti Saharom (Prai) and Cik Wati Binti Yusuf (Alor Setar) who patiently assisted me with the preparation of 5,060 sets of questionnaires to be posted to the respondents.

Also I would like to thanks Puan Suhazimah Binti Dzazali from the Malaysian Administrative Modernization and Management Planning Unit (MAMPU), Encik Shamsul Bahrim Teh Ahmad (Integrated Audio-Visual Systems Consultant) of DESD Technology (M) Sdn Bhd, Puan Lily Maria (Software Engineer) from Mesiniaga Berhad (Penang), Encik Alias Bin Yusof (ICT Security Officer) and Encik Zulham Bin Hamdan (Head of Systems Analysts) from the Centre for Knowledge, Communication and Technology, USM, Associate Professor Dr. Razak Bin Dali and his wife Puan Sharifah Shipak Bt. Tan Sri Datuk Syed Hassan Aidid, Encik Azmi Bin Salleh (Head Assistant District Officer) from the Land Office Seberang Perai Utara, Puan Nuriannahar Binti Mohamed (Director) of the Penang State Computer Centre, Encik Zainol Abidin Bin Md Noh (Council Secretary) and Mrs Lee Moong Nah (Information Technology Section Director) of the Province Municipal Council of Seberang Perai, Encik Mohd. Hornain bin Abd. Wahab (Information Section Manager) and Mr. Hira Singh a/l Gurmej Singh (MIS officer) of the Municipal Council of Penang and Mr

Leong Choon Cheong (ICT Section Manager) of the Penang Development Corporation, and many more, for their cooperation and support.

Last, but not least, to all my comrades, the 302 MIS managers and 2,441 network users respondents of the 302 Malaysian Public organizations throughout West Malaysia, I would like to thank them, May Allah bless and rewarded them for their kindness and cooperation.

TABLE OF CONTENTS

Page

CHAPTER 5 RESEARCH DESIGN AND METHODOLOGY

CHAPTER 6 DATA ANALYSIS AND FINDINGS

CHAPTER 7 DISCUSSION AND CONCLUSION

LIST OF TABLES

LIST OF FIGURES

Page

LIST OF APPENDICES

PENYALAHGUNAAN KOMPUTER , FAKTOR-FAKTOR IKATAN SOSIAL DAN PERANAN PENCEGAHAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI SEBAGAI PEMODERAT DALAM ORGANISASI-ORGANISASI AWAM MALAYSIA

ABSTRAK

Peristiwa penyalahgunaan komputer telah bertambah pada kadar yang memeranjatkan meskipun organisasi-organisasi telah berusaha dalam mengimplementasikan faktor-faktor pencegahan seperti polisi dan teknologi keselamatan teknologi maklumat dan komunikasi (ICT). Berdasarkan kepada teori ikatan sosial oleh Hirschi (1969), kajian ini mengkaji persepsi pengguna terhadap keberkesanan polisi dan teknologi keselamatan teknologi maklumat dan komunikasi (ICT), akan mengukuhkan lagi perkaitan negatif di antara faktor-faktor ikatan sosial para pengguna dengan niat para pengguna untuk menyalahgunakan komputer. Kajian ini menggunakan kaedah tinjauan dan 302 organisasi awam di Malaysia Barat telah diperolehi dengan menggunakan kaedah secara rawak. Data dikumpulkan melalui borang soalselidik yang diposkan kepada pengurus sistem maklumat (MIS) dan para pengguna rangkaian.

Kedua-dua komitmen dengan organisasi dan kepercayaan terhadap noma-norma dan nilai-nilai mempunyai perkaitan negatif dengan niat untuk menyalahgunakan perisian. Disamping itu, ikatan dengan rakan-rakan sekerja, ikatan diri dengan organisasi, perasaan kekitaan di dalam organisasi dan kepercayaan terhadap norma-norma dan nilai-nilai mempunyai perkaitan negatif dengan niat untuk menyalahgunakan rangkaian. Walaubagaimanapun, kedua-dua ikatan keluarga dan ikatan dengan pegawai atasan mempunyai perkaitan positif dengan niat untuk menyalahgunakan Internet. Ini mungkin disebabkan oleh wujudnya subbudaya yang menyeleweng (deviant) di kalangan para pengguna Internet di organisasi-organisasi awam Malaysia.

Keputusan juga menunjukkan bahawa keberkesanan teknologi keselamatan ICT menguatkan lagi perkaitan negatif di antara ikatan dengan keluarga dengan niat untuk menyalahgunakan perisian. Juga, didapati keberkesanan teknologi keselamatan ICT menguatkan lagi perkaitan negatif di antara ikatan dengan pegawai atasan dengan niat untuk menyalahgunakan rangkaian dan kepercayaan terhadap norma-norma dan nilai-nilai dengan niat untuk menyalahgunakan rangkaian. Begitu juga dengan keberkesanan polisi keselamatan ICT menguatkan lagi perkaitan negatif antara ikatan dengan pegawai atasan dengan niat untuk menyalahgunakan rangkaian, dan kepercayaan terhadap norma-norma dan nilai-nilai dengan niat untuk menyalahgunakan rangkaian. Walaubagaimanapun, kesan pemoderatan keberkesanan polisi keselamatan ICT terhadap perkaitan antara ikatan dengan keluarga dengan niat untuk menyalahgunakan Internet, telah mengakibatkan kesan berlawanan dalam mengurangkan niat para pengguna untuk menyalahgunakan Internet. Juga kesan berlawanan di dapati dengan keberkesanan teknologi keselamatan ICT sebagai pemoderat dalam perkaitan-perkaitan antara ikatan keluarga dengan niat untuk menyalahgunakan Internet, perasaan kekitaan di dalam organisasi dengan niat untuk menyalahgunakan Internet dan penglibatan tugas dengan penyalahgunaan Internet. Oleh yang demikian, terbukti daripada kajian ini mungkin akan menimbulkan minat di kalangan organisasi-organisasi Awam Malaysia untuk melihat kepada faktor-faktor ikatan sosial selain daripada pencegah-pencegah dalam usaha untuk mengurangkan penyalahgunaan komputer di kalangan para pengguna.

COMPUTER ABUSE, SOCIAL BOND FACTORS AND THE ROLE OF INFORMATION AND COMMUNICATION TECHNOLOGY DETERRENTS AS MODERATOR IN THE MALAYSIAN PUBLIC ORGANIZATIONS

ABSTRACT

Computer abuse incidents are increasing at an alarming rate despite organizations effort in implementing countermeasures such as information and communication technology (ICT) security policy and technology. Based on Hirschi’s (1969) social bond theory, this study hypothesized that users’ perception towards the effectiveness of ICT security policy and technology would strengthened the negative relationships between users’ social bond factors and users’ intention to computer abuse. A survey method was employed and a sample size of 302 public organizations in West Malaysia was randomly selected. Data was collected through mailed questionnaires to both MIS managers and network users. Both commitment to organizations, and belief in norms and values are found to have negative impact on intention to software abuse. In addition to that, attachment to co-workers, personal attachment to organizations, sense of belonging in organizations and belief in norms and values are found to have negative impact on intention to network abuse. However, both attachment to families and attachment to immediate supervisors have positive impact on intention to the Internet abuse. These could be due to the fact that there may in existence be a deviance subculture among the Internet users in the Malaysian Public organizations.

Results have shown that, ICT security technology effectiveness strengthened the negative relationship between attachment to families and intention to software abuse. Also, it was found that ICT security technology strengthened the negative relationships between attachment to immediate supervisors and intention to network abuse, and belief in norms and values and intention to network abuse. Likewise, it was also found that ICT security policy effectiveness strengthened the negative relationships between attachment to immediate supervisors and intention to network abuse, and belief in norms and values and intention to network abuse. On contrary, the moderating effect of ICT security policy effectiveness on the relationship between attachment to families and intention to the Internet abuse has resulted in an adverse effect in reducing users' intention to the Internet abuse. Similar adverse effect with ICT security technology effectiveness as moderator has also been observed on the relationships between attachment to families and intention to the Internet abuse, sense of belonging in organizations and intention to the Internet abuse, and job involvement and intention to the Internet abuse. Therefore, as evidence by this study may create interest among the Malaysian Public organizations to look at users' social bond factors besides deterrents in an endeavor to reduce users' computer abuse.

CHAPTER 1

INTRODUCTION

This chapter provides a background to the research. It explores the problem statement, research questions, research objectives, research scope, the significance of the study, and the definitions of variables are provided at the end of the chapter.

1.0 Background of the Study

Computer systems have moved from applications for back-office support to those offering significant competitive advantage because of its great speed and the sharp reduction in the cost of information systems (IS) technology (McFarland, 1984). In addition to that, the quality and awareness of computer applications using network and Internet environment are increasing among organizations. According to Anandarajan, Simmers and Igbaria (2000), the Internet is having a critical role in helping many organizations to reduce costs, shorten product cycle times, and market products and services more effectively.

These have generated a very high demand for information and communication technology (ICT) acquisition and implementation among organizations (Bidgoli & Azarmsa, 1989). For examples, the total number of personal computers (million units installed) in Malaysia has increased from 0.61 in year 1995 to 5.7 in year 2005 and it was forecasted to be 11.5 for year 2010. The total number of dial-up Internet subscribers (million) has increased from 0.04 in year 1995 to 13.9 in year 2005 and it was forecasted to be 10.0 for year 2010. The total number of Internet broadband subscriptions (million) was 0.49 in year 2005 and was forecasted to be 3.73 for year 2010. The total number of Internet users (million) has increased from 0.03 in year 1995 to 8.19 in year 2003 (Government of Malaysia, 2006).

In line with this, the Government of Malaysia has taken drastic actions to develop the national ICT infrastructures and applications and this include the civil service management and administrative reforms through the increasingly widespread use of information technology. The government's attention will continue to be focused on expanding the use of the latest technology, in the overall effort towards achieving a paperless Civil Service, and the implementation of Electronic Government as part of the Multimedia Super Corridor (MSC) development. The government has taken active roles in bringing the country into the Information Age. Electronic Government is one of the MSC Flagship Application applying Multimedia technologies to improve the government's operations (Ali, 1997). In relation to this, the Government of Malaysia has increased its expenditure on ICT over the years, i.e. from RM1,389 million in year 2000 to RM2,245 million in year 2005 and a total of RM12.9 billion is allocated for ICT-related projects for the Ninth Malaysian Plan (Government of Malaysia, 2006).

As the country expands its computerization agenda, employees are encountering more unethical attractive situations than ever when using a computer (Gattiker & Kelley, 1999). According to Lim, Teo and Loo (2002) and Lim (2002), it is also recognized, that the Internet serves as a double-edge sword for organizations in that it opens up new opportunities for employees to cyberloaf on the job. According to Straub and Nance (1990), Cappel and Windsor (1998), Marshall (1999) and Cronan and Douglas (2006), in spite of its undoubted value to users and organizations, information technology (IT) poses some risks and ethical issues, because of its misuse results in losses to business (economy), society and the IT profession.

In contrast to the general perception that computer abuse is committed by external hackers, the majority (60%) of computer abuse is actually done by users within organizations (Computer Security Institute/Federal Bureau of Investigation, 2001) and

70 – 80% of security incidents are caused by insiders (Richards, 2004). In fact, Olson and Olson (2000) pointed out that the primary threat of security breaches actually originated from within the organizations.

The number of computer abuses cases reported in Malaysia has increased from 155 cases from the period of August – December, 1997 to 20,542 cases for the period of January to June, 2007 (National ICT Security And Emergency Response Centre, 2007) as depicted on Figure 1.1 and Figure 1.2.

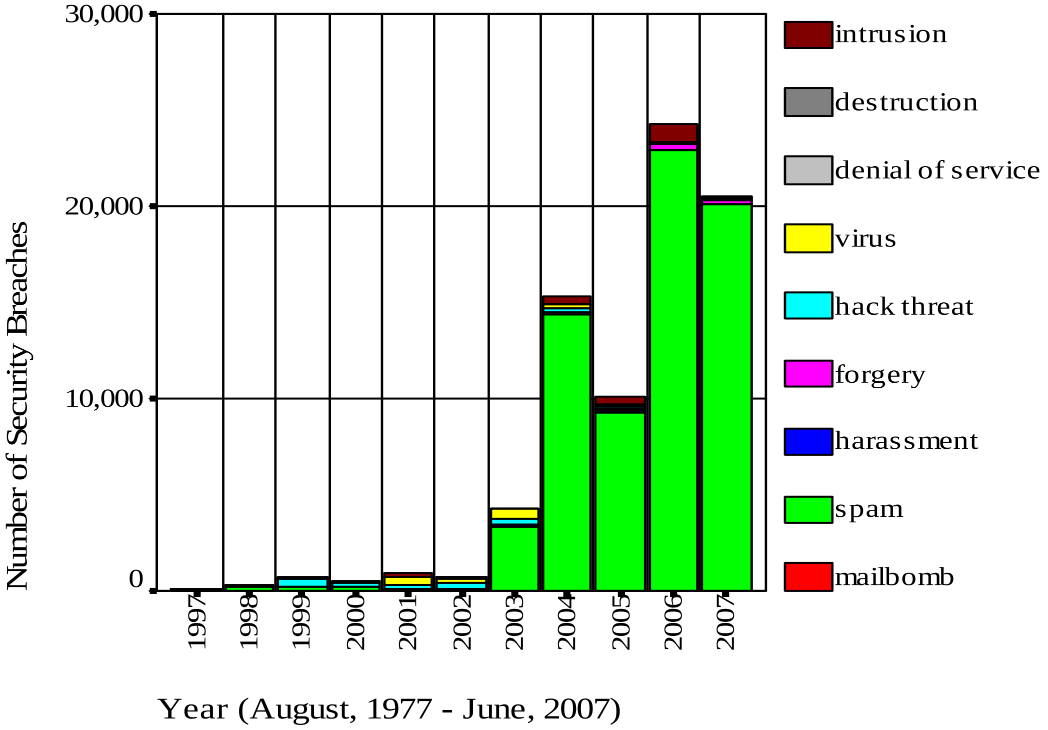

Figure 1.1 Number of computer abuse incidents from August, 1997 – June, 2007.

Computer abuse incidents in public organizations could disrupt Government mission in providing the best service to its stakeholders that include the business organizations and the public, which in turn will affect the activities of business organizations. According to Coccia (1998), when normal work behaviour goes outside the norms of the organization, its consequences are far-reaching and affect all levels of the organization including its' decision-making processes, productivity and financial costs. Purdham (2005) pointed out that the downloading and viewing of pornography at work is likely to reduce productivity, damage staff morale and expose organizations to a myriad of different legal risks. Suhail and Bargees (2006) conducted a study to investigate the positive and negative effects of excessive Internet use on undergraduate students. They found that excessive Internet use can lead to a host of problems of educational, physical, psychological and interpersonal nature.

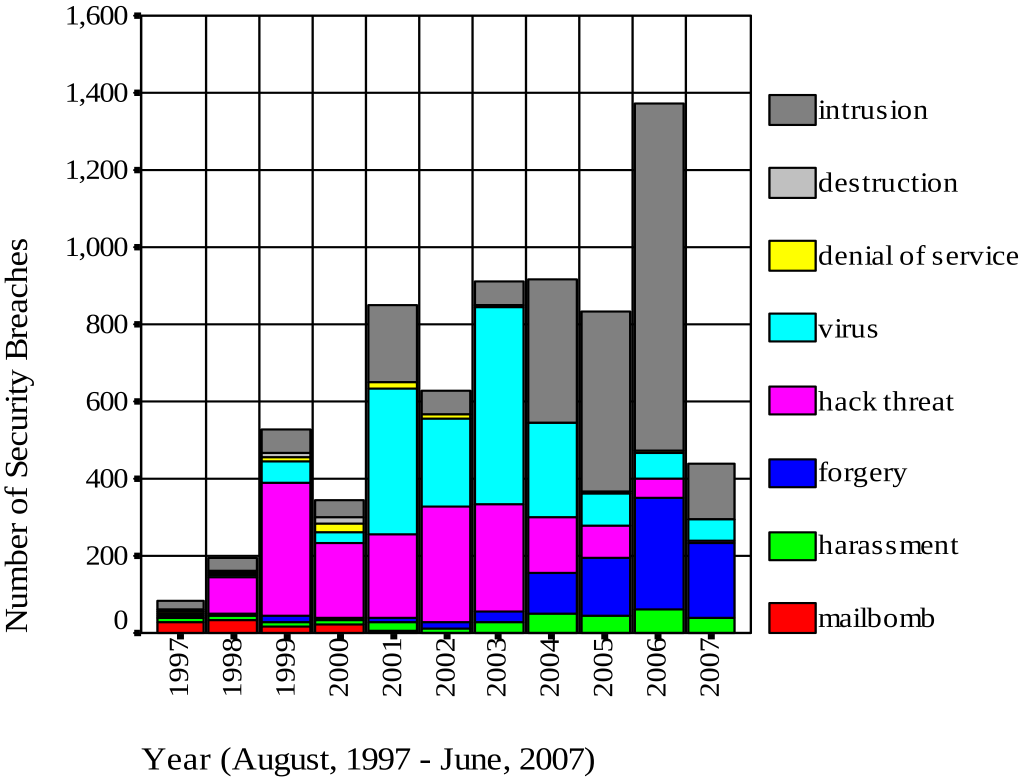

Figure 1.2 Security breaches (excluding spam) from August, 1997 – May, 2007.

Thus, computer abuse is a management problem because of its adverse effect on the organizations in terms of system damaged, productivity loss, financial and time loss, and legal implication.

Computer abuses incidents could result in damage to the organization's computer system (New Straits Time, 1997) and serious loss of data including lose of data completely (Malaysian Computer Emergency Response Team, 2001). It could also jeopardize the organization’s network traffic and halted the operation of the all production systems. According to the National ICT Security and Emergency Response Centre (2003), with an ever-increasing business reliance on information technology, a key issue is not only how best to minimize disruption, but also on how quickly and effectively normal operations can be restored when disruption occurs. From the National ICT Security and Emergency Response Centre (2003) ICT security survey for Malaysia 2001/2002, 33.4% of organizations which suffered ICT security breaches were able to restore business operations within a day, followed by a third who took up to a week. Only 4% of organizations took more than a week to get business operations back to normal, while the other 25% reported that the incident did not affect their business operations at all (National ICT Security and Emergency Response Centre, 2003).

Productivity loss is both insidious and pervasive when employee’s access personal e-mail, surf pornography, sports, shopping and personal finance web sites, instant messaging, online games and downloading of MP3 and video files (Keong, 2005). Directly linked to the productivity issue is efficient utilization of computing resources. For organizations, the potential negative impacts from lost of productivity alone represents a multibillion-dollar issue. In 1999, companies in U.S. lost RM20.14 billion to recreational Internet surfing by employees (Keong, 2005). If Internet abuse by staff is left unchecked, it could easily turn into an epidemic pattern of abuse, making it a norm. Unproductive Internet use consumes valuable processing power, memory, disk space and bandwidth (Keong, 2005).

Staff abusing their Internet access privileges could reduce the organization network bandwidth, degraded system performance, and over consumption of finite ICT resources, which could indirectly lower down the productivity of other non-abusing users (Stewart, 2000). When the organization network performance is downgraded, organizations are often been forced to respond with major new investments system improvements and bandwidth expansion, even though they may not be aware that a significant part of the network demand was a result of inappropriate Internet usage by staff (Stewart, 2000). And organizations are often forced to respond to such bottlenecks by putting in expensive system or connection upgrades (Keong, 2005).

Studies from the U.S. Department of Labor have shown that the productivity of the U.S. workers have abruptly declined due to employees' inappropriate use of corporate Internet connections to view inappropriate material, gamble online, download music, conduct personal shopping, trade stocks and conversing through instant messenger programs (CyberDefense, 2004). Based on an extensive study conducted by Vault.com, over half of the employers surveyed believe that employees surfing non-work related web sites compromises employee productivity (CyberDefense, 2004). Ramayah and Baharudin (2005) have also conducted a research on personal Web usage among employees working in the Penang Free Trade Zone with access to the Internet at the workplace. They found that the extent of personal downloading, personal information research and personal e-commerce were positively associated to work inefficiency whereas personal communication was not significantly related to work inefficiency. In addition to that, Caplan (2005) in his study integrates research on social skill and self-presentation into cognitive-behavioral theory of generalized problematic Internet use. He found that compulsive Internet use was positively associated with negative outcomes of Internet use.

The consequence from the high computer abuse incidents has resulted in the government increased expenditure on ICT including to eradicate the damaged done by computer abuse. The National ICT Security And Emergency Response Centre ICT

Security Survey for Malaysia 2000/2001 (participation from 205 organizations) revealed that 205 participative Malaysian organizations suffered a total of RM43.8 million (employees' abuse from downloading pornography), RM1.04 million (employees' abuse from inappropriate use of e-mail system), RM4.2 million (employees' abuse from installing pirated software), RM820,000 (sabotage of data or network) and RM514,960 (website vandalism & unauthorized access/misuse) in the year 2000 (National ICT Security And Emergency Response Centre, 2003).

From the CMP Business Media Ptd Ltd (2003) Asian Computer Crime 2003 Survey, out of 1,064 respondents who indicated that they are the victims to computer abuse, only 410 (38.5%) were able to quantify their losses. This suggests that many Asian companies have no means of accounting for computer abuse losses in their companies and this will have an adverse impact on the accuracy of security budgets that IT managers will draw to combat computer abuses in future.

As reported by 490 companies participated in the Computer Security Institute/Federal Bureau of Investigation (CSI/FBI) (2003) Computer Crime and Survey 2003, a total of USD201.8 million of annual losses was reported for the year 2003 as compared to USD455 million reported in 2002. In terms of severity of losses for the year 2003, theft of proprietary information caused the greatest financial loss of USD70.2 million. Losses due to financial fraud were drastically reduced for the year 2003, at USD10.2 million as compared to nearly USD116 million for the year 2002. Companies which suffered denial of service attacks with losses of USD65.7 million for year 2003.

According to the Computer Security Institute/Federal Bureau of Investigation (CSI/FBI) (2004) Computer Crime and Survey 2004 which was participated by 269 companies, amount of losses by type; USD10.6 million (insider net abuse), USD10.2

million (abuse of wireless network), USD.8 million (misuse of public web application) and USD4.3 million (unauthorized access).

In terms of legal liabilities, employers could potentially be held liable for their staff that uses organization Internet connections to violate copyright laws or to post false information that libels other organizations or individuals. Organizations could be deemed responsible for illegal activities, for example fraudulent Internet scams, conducted by their employees if it involved the organizations equipment and Internet access. In addition to wasting company time and money, this behavior also placed employers at potential risk for lawsuits and negative publicity. Organization too could sustain significant damage to its reputation and goodwill as a result of the negative publicity that can ensue from staff misuse of the Internet (Stewart, 2000).

In Malaysia, cyber laws form an important component of the legal framework needed to facilitate the development of ICT systems by countering the threats and abuses related to such systems (Government of Malaysia, 2002b). The cyber laws are Digital Signature Act 1997, Computer Crime Act 1997, Telemedicine Act 1997, Copyright (Amendment) Act 1997, Communications & Multimedia Act 1998, and Malaysian Communications & Multimedia Commission Act 1998. In addition other existing regulations, which are related to computer crime include Copyright Act 1987, Official Secrets Act 1972, Companies Act 1965 (Act 125), Trade Marks Act 1976, Patents Act 1983, Prison Act 1995, National Archives Act 2003, and Defamation Act 1957 (Act 286).

In addition to Cyber Law, organizations could take disciplinary action against staff misusing Internet. Under Clause (2) Article 132 of the Federal Constitution Section 4(2), an officer shall not be inefficient, dishonest, irresponsible, disobey direction and negligent when carrying his or her duty. Any violations of the Section 4(2) Clause (2)

Article 132 of the Federal Constitution, the officer could be charge by their respective organizations under disciplinary action as laid down by the General Circular Chapter D (Law Research Board, 2005).

The growing variety of security threats combined with an increasing number of geographical interconnected systems and virtual offices have made the management of employee attitudes toward security a paramount concern (Andress & Fonsecca, 2000). Security leaders have a choice either to manage their own backyard more carefully, or pay the price (Andress & Fonsecca, 2000).

Because of the negative consequences of computer abuse to organizations, computer security thus has become a managerial problem as well as a technical one, a development which has a dramatic impact on the success and/or failure of any computer utilization (Bidgoli & Azarmsa, 1989). Protection from security breaches requires investment in technology, services, and personnel as well as adjustments in corporate culture (Breidenbach, 2000). Researchers such as Straub (1989, 1990), Straub and Collins (1990) and Mirchandani and Motwani (2003) have applied the general deterrence theory (GDT) proposed by Beccaria in 1959 which stated that countermeasures such as ICT security policy and ICT security technology could reduce computer abuse incidents.

As such, the Malaysian public organizations sought to deterrent countermeasures such as ICT security technology and ICT security policy to combat computer abuse by their users. On average Malaysian organizations has invested about RM120,000 in 2000 and RM343,527 in 2001 for ICT security system (National ICT Security And Emergency Response Centre, 2003) (see Figure 1.3).

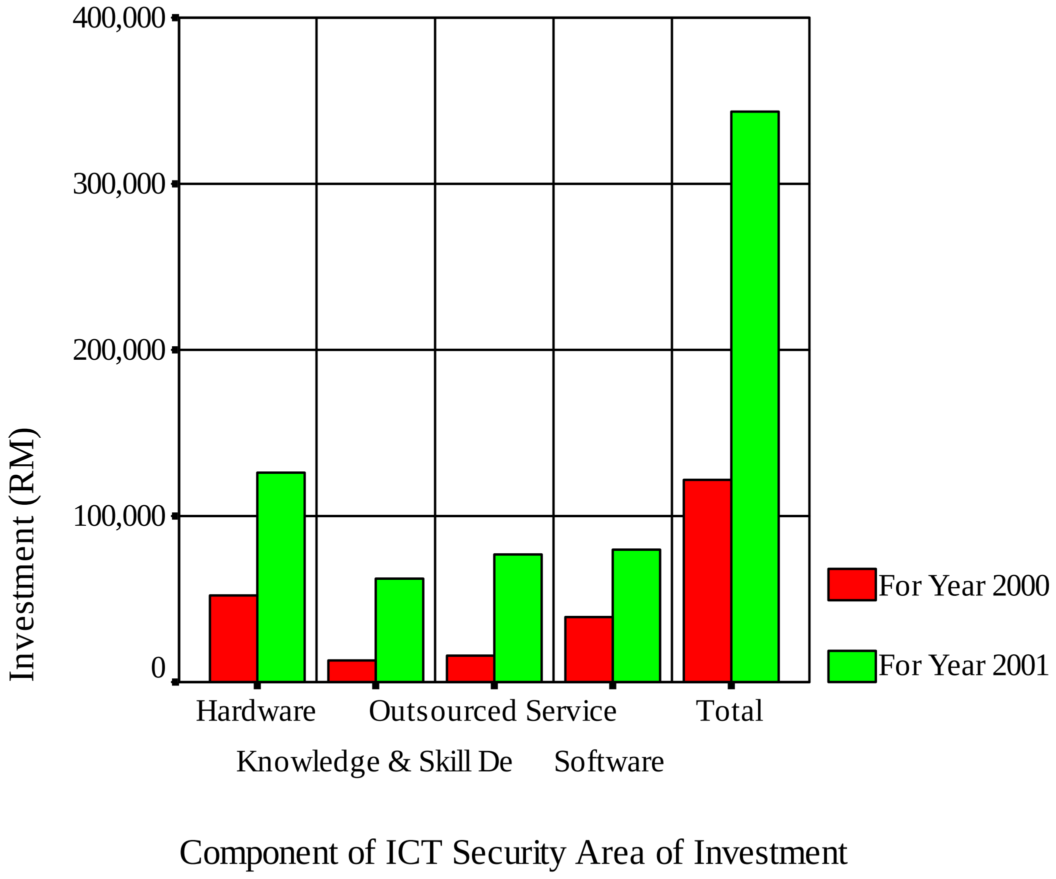

Figure 1.3 Investments on ICT security system in the years 2000 and 2001.

In addition to that, the Government of Malaysia has issued various circulars on ICT security policy, procedures and guidelines to its agencies so as to protect their computer resources against security breaches (Government of Malaysia, 2002b).

Despite the investment in countermeasures, the computer abuse incidents are still increasing at an alarming rate in the Malaysian public organizations. Figure 1.4 and Figure 1.5, show that for the period from July, 2006 to June, 2007; there were harassment (79 cases), forgery (335 cases), hack threat (42 cases), malicious code (76 cases), denial of service (6 cases), intrusion (671 cases) and spam (35,930 cases)(National ICT Security And Emergency Response Centre, 2007).

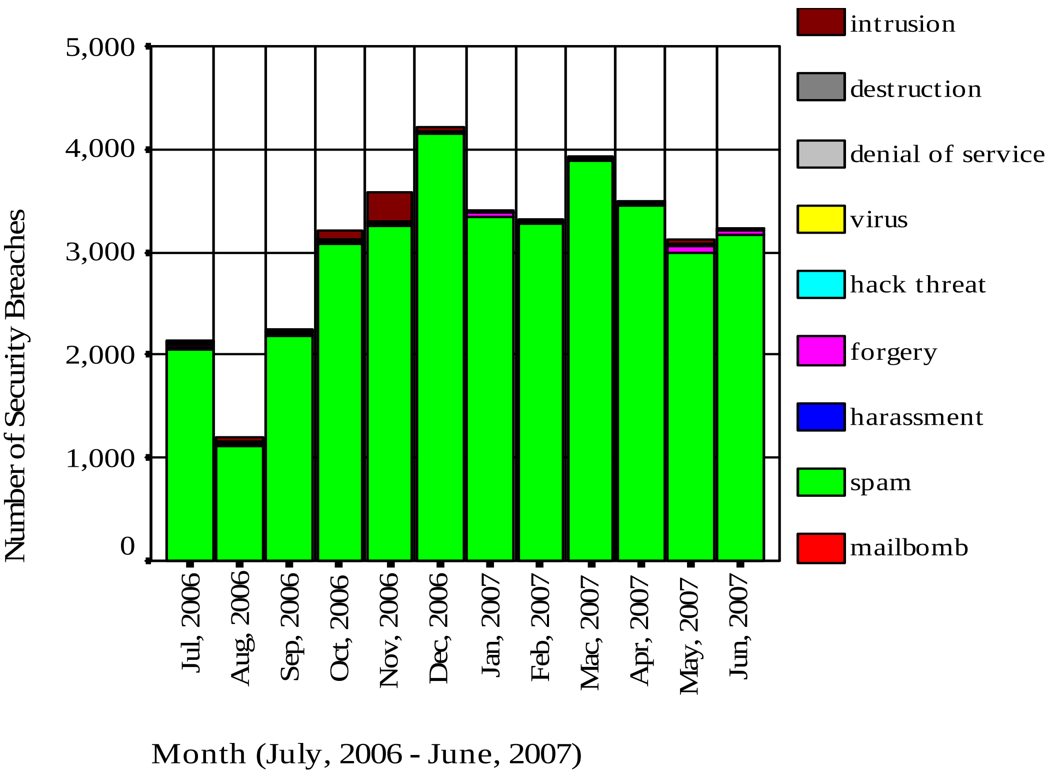

Figure 1.4 Security breaches for the period of July, 2006 – June, 2007.

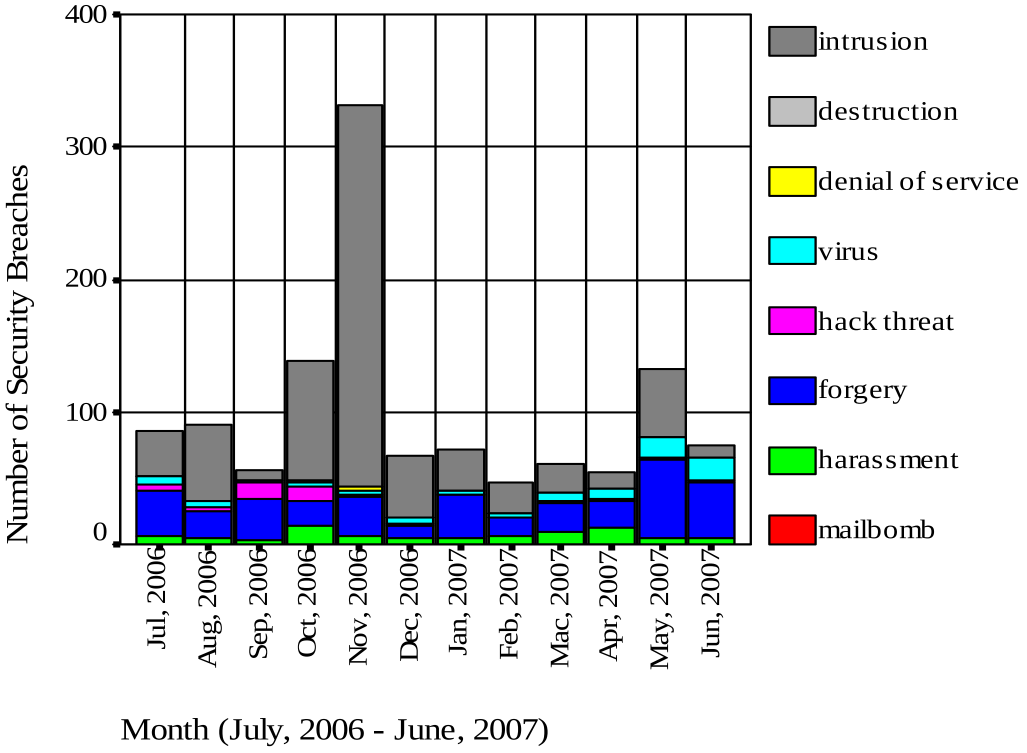

Figure 1.5 Security breaches (excluding spam) for the period of July, 2006 – June, 2007.

Why has computer abuse not been reduced? Nowadays, researchers doubt that previous general deterrent theory (GDT)-based research adequately explains the current phenomenon of computer abuse occurring inside organizations. The present GDT explains how security measures implemented by organizations rely solely on technology without considering other factors, such as people and processes (Lee, Lee & Yoo, 2004). For example, Straub (1989, 1990) stated that security countermeasures which include deterrent administrative procedures and preventive security software resulted in significantly lower computer abuse. However, Straub did not include another piece of the security puzzle, the human dimension. Thus, the need for understanding computer abuse with a different approach other than the traditional GDT has arisen.

However, this research provide an alternative theoretical framework to tackle the issue of users' computer abuse in the Malaysian public organizations by looking into the social aspect by adopting the social bond factors rather than focusing merely on deterrent variables such countermeasures. Social bond theory (SBT) attribute the deviant acts to social relationships of individuals have received considerable attention by researchers in criminology and sociology that views the deviant act as a result of the weakness or inexistence of social bonds of the individual.

ICT security is the process of protecting data from unauthorized access, use, disclosure, destruction, modification, or disruption (Cornell University, 2007; Wikipedia, 2007). It consists of efforts to ensure that the organization's computer assets which include hardware, software (programs, data and information) and human ware are protected against threats and abuses. It consists of both the hard part (Straub 1989, 1990) and the soft part (Lee & Lee, 2002; Lee, Lee & Yoo, 2004; Lee, Nah & Yoo, 2001) of security efforts to overcome computer abuse or threat. The hard part of security effort include countermeasures such as ICT security technology and policies (Straub 1989,

1990) and the soft part of the security effort include the social bond factors such as users' attachment to significant others, users' attachment to the organization, users' commitment to the organization, users' job involvement and users' belief in norms and values (Hirschi, 1969; Lee & Lee, 2002; Lee, Lee & Yoo, 2004; Lee, Nah & Yoo, 2001). By managing both the hard and soft parts of the security effort, organizations could reduce security threats or abuses (Hirschi, 1969; Lee & Lee, 2002; Lee, Lee & Yoo, 2004; Lee, Nah & Yoo, 2001; Straub 1989; 1990).

Thus the impact of users' social bond factors on users' intention to computer abuse and the moderating effect of ICT security policy and technology effectiveness on the relationship between users' social bond factors and users' intention to computer abuse in the Malaysian public organizations are investigated in this research.

1.1 Problem Statement

Hence, this study will investigate the impact of users' social bond factors namely attachment to people in terms of work-related relationship between users and families, immediate supervisors, co-workers and friends outside work, users' attachment to the organizations, users' commitment to the organizations, users' job involvement and users' belief with norms and values, on users' intention to computer abuse in the Malaysian public organizations. In addition to that, this study will also investigate whether deterrent variable namely; users' perception towards the effectiveness ICT security policy and ICT security technology in the organization strengthened the negative relationship between users' social bond factors and users' intention to computer abuse.

1.2 Research Objectives

The following objectives frame this study:

a. To determine the extent of computer abuse in the Malaysian public organizations.

b. To investigate the relationship between users' social bond factors and users' intention to computer abuse.

c. To investigate whether users' perception towards deterrents effectiveness in the organization moderate the relationship between users' social bond factors and users' intention to computer abuse.

1.3 Research Questions

From the above discussions, the research questions stated in this study are:

a. What is the extent of computer abuse in the Malaysian public organizations?

b. What is there a relationship between users' social bond factors and users' intention to computer abuse?

c. Does users' perception towards the effectiveness of ICT security policy in the organization moderate the relationship between users' social bond factors and users' intention to computer abuse?

d. Does users' perception towards the effectiveness of ICT security technology in the organization moderate the relationship between users' social bond factors and users' intention to computer abuse?

1.4 Research Scope

The scope of this research is computer abuses that occur in the Malaysian public work places whereby their users (insiders) who have access to the Internet causing security breaches in the organization. Public sector includes the ministries, state governments, federal government departments, state government departments, federal statutory bodies, state statutory bodies, local governments and city councils. Computer abuse committed by users (insiders) include Internet abuse (personal usage of office e-mail, chatting, non-work related Internet browsing, and downloading of files), software abuse (non license software usage), and network abuse (intrusion).

1.5 Significance of the Study

The proposed research model will contribute to the theoretical body of knowledge about users' computer abuse in the Malaysian public organization by providing a new angle for attacking the problem through the modified social-technical perspective, rather than the pure social or pure technical approaches.

This study contribute to the theoretical body of knowledge in terms of the dimensions for users' intention to computer abuse (dependent variable), users' attachment to others (independent variable) and users' attachment to the organization (independent variable). From the factor analyses, three dimensions of users' intention to computer abuse emerged (users' intention to the Internet abuse, users' intention to software abuse and users' intention to network abuse) instead of one dimension proposed by previous researchers. Three dimensions of users' attachment to others (users' attachment to family, users' attachment to immediate supervisors and users' attachment to co-workers) were found, whereas previous researchers found only one dimension. Two dimensions of users' attachment to the organization (users' personal attachment and users' feeling sense of belonging) were yielded although previous researchers applied only one dimension.

Theoretical contribution of this study also include the measurements used for users' intention to computer abuse (dependent variable), users' perception towards the effectiveness of ICT security policy and users' perception towards the effectiveness of ICT security technology in the organization. Four self-construct items were introduced with respect to users' intention to computer abuse and all the items used to measure both users' perception towards the effectiveness of ICT security policy and users' perception towards the effectiveness of ICT security technology in the organization were self-construct items.

Also contribution of this study comes from the introduction of deterrent (users' perception towards the effectiveness of ICT security policy and users' perception towards the effectiveness of ICT security technology in the organization) as the moderator to the relationship between users' social bond factors and users' intention to computer abuse. However, previous researchers treated deterrent and social bond factors as independent variables to users' intention to computer abuse. Also the definitions for the moderating variables are an added contribution. For the purpose of this study deterrent was defined as users' perception towards the effectiveness of ICT security policy and technology rather than been treated as just 'hard technology' per se by previous researchers.

In addition to that, the introduction of organization as unit of analysis is an added contribution of this study, unlike the previous researchers who treated either individual or abuse incidents as the unit of analysis. While the application of the social bond theory to explain the moderating effect of deterrents on the negative relationship between users' social bond factors and users' intention to computer abuse is a further contribution of this study. However, previous researchers applied the social bond theory to explain the relationship between users' social bond factors and users' intention to computer abuse, while the general deterrence theory was used to explain the relationship between deterrent and users' intention to computer abuse. The detailed discussion on the theoretical contribution of this study is given in section 7.8 of Chapter 7.

The practical significance of this study lies in its attempt to provide a framework for reducing users' intention to computer abuse in the Malaysian public organizations by management of users' social bond factors. The study will benefit the management of public organization by the enhancement of users' social bonds factors and to minimized users' computer abuse. In addition to that, this research would be valuable to the Malaysian public organizations when dealing with computer abuse, they should look at the moderating effect of deterrents such as users' perception towards the effectiveness of ICT security policy and users' perception towards the effectiveness of ICT security technology on the relationship between user's social bond factors and users' intention to computer abuse. Thus, to address the issue of computer abuse, government and management of public organizations need to focus on users' social bond variables and to take the necessary steps and actions to improve users social bond factors so as to minimize the abuse phenomena at public work place, rather than merely investing and reinvesting in countermeasures such as ICT security policy and ICT security technology.

Last but not least, this study will provide empirical data to investigate the current level of users' computer abuse and users' intention to computer abuse in the Malaysian public organizations. The detailed discussion on the theoretical contribution of this study is given in section 7.7 of Chapter 7.

1.6 Definitions of Variables

Users' Computer Abuse is defined as the frequency of security violation incident (Straub, 1990) committed by users that occur in the organization which is related to software abuse (non-license software usage), Internet abuse (personal e-mail usage, chatting, non-work related Internet browsing, downloading of files) and network abuse (intrusion).

Users' Actual Internet Abuse is defined as the frequency (weekly average for the past three years) users engagement in the Internet abuse activities such personal e-mail usages, non-work related Internet chatting, Internet surfing, and downloading of files from the Internet at the work place.

Users' Actual Software Abuse is defined as the frequency (weekly average for the past three years) user's engagement in the usage of non-license of commercially sold software with the computers at the work place.

Users' Actual Network Abuse is defined as the frequency (weekly average for the past three years) user's engagement in the intrusion of the organizations' systems using the computers at the work place.

Users' Intention to Computer Abuse is defined as the extent to which users' intent to commit computer abuse in the work place which is related to software abuse (non-license software usage), E-mail abuse (personal e-mail usage) and network abuse (chatting, non-work related Internet browsing, downloading of files, intrusion).

Users' Intention to Internet abuse is defined as the extent to which users' intent to commit Internet abuse at the work place which is related to personnel e-mail usage, non-work related Internet chatting, Internet surfing, and downloading of files.

Users' Intention to software abuse is defined as the extent to which users' intent to commit software abuse at the work place which is related to using non-license of commercially sold software with the computers in the organization.

Users' Intention to network abuse is defined as the extent to which users' intent to commit network abuse at the work place which is related to intrusion of the organizations system.

Users' Attachment to Persons (people) is referred to as the extent to which there is helping relationships (work-related assistance) that exist between users and significant others (family, the immediate supervisor, and co-workers (peers) and friends outside work) (Hirschi, 1969; Kim, 1996).

Users' Attachment to their Families is defined as the extent to which there is helping relationship (work-related assistance) that exist between users and their families members (spouse or parent) (Hirschi, 1969; Kim, 1996).

Users' Attachment to their Immediate Supervisors is defined as the extent to which there is helping relationship (work-related assistance) that exist between users and their immediate supervisors (Hirschi, 1969; Kim, 1996).

Users' Attachment to their Co-workers is defined as the extent to which there is helping relationship (work-related assistance) that exist between users and their co-workers (friends) (Hirschi, 1969; Kim, 1996).

Users' Attachment to the Organization is referred to as the extent of users' affective commitment towards the organization. It is the extent to which users perceive that they are personally attached to, identification with, and involvement in, the organization (Hirschi, 1969; Meyer, Allen & Smth, 1993).

Users' Personal Attachment to the Organization is referred to as the extent of to which users are personally attached to or feeling of affection towards the organization.

Users' Sense of Belonging in the Organization is referred to as the extent of users feeling emotionally attached as being part of the members in the organization.

Users' Commitment to the Organization is referred to as the extent of users' continuance commitment towards the organization. It is the extent to which users' perceived cost associated with leaving the organization (Meyer, Allen & Smith, 1993).

Users' Job Involvement is referred to as the extent to which users' are engaged in the specific tasks that makes up users' job (Paullay, Alliger & Stone-Romero, 1994).

Users' Belief in Norms and Values is referred to as the extent to which users' endorsement of values and norms (Hirschi, 1969). Norms are expectations or rules in the organization shared by a group members of how they ought to behave under a given set of circumstances (Shani & Lau, 1996).

Users' Perception towards the Effectiveness of ICT Security Policy in the Organization is referred to as the users' perception on the extent of the ICT security policy effectiveness in deterring users from abusing the computer in terms of user's awareness about the appropriate and inappropriate uses of the computer, about the types of disciplinary action as consequences of purposeful computer abuse, the overall security philosophy of the organization and the perception about the activities of computer security administrators (Straub 1989, 1990).

Users' Perception towards the Effectiveness of ICT Security Technology in the Organization is referred to as the users' perception on the extent of the ICT security technology effectiveness is effective in protecting the computer resources in terms of confidentiality, integrity, availability and accountability (Fraser, 1997; Government of Malaysia, 2002b; State of Texas Department of Information Research, 2001).

1.7 Organization of the Thesis

The thesis is organized into seven chapters. This chapter provides the research background, the problem statement, research questions, research objectives, the significance of the study, the scope of the study, and the definitions of key terms. Chapter 2 discusses a preliminary study which was conducted by interviewing various personnel which include the MIS managers, ICT security officer, systems analysts and users from five public organizations that include two federal statutory bodies, one state statutory body and two local governments in order to understand the phenomena of computer abuse in the public sector.

Chapter 3 elaborates a review of literatures which highlights key previous studies related to users’ computer abuse, users’ intention to computer abuse, users’ attachment to people, users’ attachment to the organization, users’ commitment to the organization, users’ job involvement, users’ belief in norms and values, users’ perception towards the effectiveness of both ICT security policy and technology in the organization. The discussion is comprised of the setting-up of concept, variables and terminology used. Chapter 4 discusses the theoretical framework, its foundation and to integrate concepts and research findings relevant to computer abuse, and hypotheses formulation. Chapter 5 discusses the research design and methodology used in testing the hypotheses, the research approach, sampling design, questionnaire development, data collection, and methods of data analyses. Chapter 6 discusses the data analyses, the revised research model and reports findings results. Chapter 7 provides the discussions on the results, limitations, implications, future research directions and conclusion.

CHAPTER 2

COMPUTER ABUSE IN PUBLIC WORK PLACES

2.0 Introduction

In order to understand the phenomena of computer abuse in the public sector a preliminary study was undertaken by interviewing the respective computer directors, managers, head of the computer sections, system analysts and users from the respective five public organizations that includes two federal statutory bodies, one state statutory body and two local governments using a semi-structured questionnaire. Details of the outcome from these interviews are given next.

A preliminary study on computer abuse was undertaken based on Preston (1991) who argued that the way management of information system (MIS) field defines "problem" is actually not true of what is actually happening out there in the real world. This is because the field of MIS has brought along the ontological, epistemological and behavioral assumptions from a number of other disciplines including from the areas of operation research, science, mathematics, statistics, cybernetics and engineering into its theoretical framework without careful reflection upon its historical emergence of these assumptions or without careful reflection upon the organizational context. In fact, Beatty (1998) reported that Porter in an interview has commented that we are living in a society of organizations which we knew very little. Thus, in order to study these organizations, one needed to be inside the organizations as a human, social, political organization – as an integrating mechanism.

Therefore in this research interviews were held with the relevant officers of five public organizations using a semi-structured questionnaire in order to understand the computer abuse phenomena in the real world.

2.1 Interviews with Organization “A”

Organization “A” is a public university that is involved in providing tertiary education in the country. It is formed under a resolution that was passed at the State Assembly in 1962. The university is headed by the vice chancellor. The computer centre of this university is responsible for all matters pertaining to the information and communication technology (ICT) planning, development, operation and maintenance including the ICT security of the university. The computer centre is headed by the chief information officer (CIO). The information and communication technology security officer (ICTSO) is responsible for the security of the university’s ICT. The computer center consists of CIO, ICTSO who is also the director of the computer center, six heads of system analyst, 30 system analysts, five senior programmers, 20 programmers and 10 computer technicians. The CIO reports directly to the vice chancellor (VC).

An interview was conducted with the ICTSO on 4th November, 2003 and two interviews were conducted with the head of system analysts on 13th October, 2003 and the 4th November, 2003 respectively. Detailed outcomes from these interviews are discussed next. According to the ICTSO, there are more than 3,000 units of personal computers (PCs) which are connected to the university’s network which are registered with the Computer Center. However, there are many PCs which were bought directly by the schools under project fund, and some which are brought along by the students, staff and faculty members including wireless notebooks which could also be connected by users to the network at each school. Most of the computer abuse originated from internal users which is difficult to control by the computer center. However, the computer center is proposing to the VC that all PCs in the campus must be registered by their media access control (MAC) addresses which are attached to each of the respective PC network card and each user will be given user identification (id) before they are allowed to use the network. MAC address is a hardware address that uniquely identifies each node of a network. Only registered PCs authenticated by their MAC addresses and user identifications (ids) will be allowed to use the network and the Internet.

According to the interviewee, although the computer centre has installed the latest ICT security technology that is available in the market, users who formed the big mass of people are still abusing the network. ICT security technology alone could not stop computer abuse altogether. It is the peoples (users) irresponsible behavior which is the main cause to computer abuse in the campus. In addition to that, the university needs a group of people, or a committee to manage ICT security issues and to create security awareness to users so as to be more responsible campus citizens.

Thus, computer abuse is mainly due to users' misbehavior, whereas ICT security technology and security policy are just tools to facilitate the control on computer abuse. Some users abuse the system by taking advantage of the loop holes that exists in the current system. For example, when Microsoft Windows 2000 initially installed with patch 2, later when patches 4 and 5 came out, computer center's personnel need to upgrade all the PCs' operating system (OS) with these patches, otherwise hackers could use this weakness to enter into the system. Hackers find that it's a challenge to penetrate popular operating systems and software.

Ninety percent (90%) of the organization's internet bandwidth are consumed by users (insiders) who abuse the organization's computers in non-work related activities such as hacking (intrusion), Internet chatting, non work-related Internet surfing including pornographic web sites and poison pen-letter (surat layang). Very soon, ICTSO will form an ICT Security Committee to manage all ICT security issues. This committee will monitor the progress/report on security issues. Currently the university has an Information Technology (IT) Council to monitor all ICT projects; below this