*Akademika 82(1) 2012: 125-137*

**Nota Penyelidikan / *Research Notes***

# Information Communications and Technology (ICT) Abuse in the Malaysian Public Sector: The Influence of Ethical, Organisational Bond and General Deterrence Factors

## Salah Guna Teknologi dan Komunikasi Informasi (ICT) dalam Sektor Awam Malaysia: Pengaruh Faktor Etika, Ikatan Organisasi dan Pencegahan Umum

Sapiah Sakri, Juhana Salim & Tengku Mohammed Tengku Sembok

ABSTRACT

*Despite continuous effort to reduce ICT abuse, ICT security problems still persist such that ICT security experts and practitioners are kept struggling to find ways to combat the problems which are closely related to deviant human behaviour. Previous studies have investigated the causal relationships between security efforts and ICT abuse but studies on ICT abuse in the Malaysian public sector are still rare. This research aims at identifying significant factors that influence ICT abuse as an input to develop and validate an ICT abuse model within the Malaysian public sector setting. The proposed model contributes to the theoretical body of knowledge on ICT abuse by adopting multi-disciplinary solutions whereby ethical factors from the discipline of psychology, organisational bond factors from the discipline of socio-criminology and general deterrence factors from the discipline of ICT security are examined and synthesised.*

*Keywords: Ethical factors, ICT abuse, ICT security problems, multi-disciplinary solutions, socio-criminology*

ABSTRAK

*Walaupun pelbagai usaha untuk mengurangkan perilaku salah guna ICT telah diambil, namun masalah keselamatan ICT ini masih terus berlaku. Oleh itu, kebanyakan pakar dan pengamal keselamatan ICT sedaya upaya mencari jalan untuk mengurangkan masalah yang berkait rapat dengan perilaku tidak lazim manusia. Kajian lampau telah menyelidiki perhubungan sebab di antara usaha-usaha keselamatan dengan perilaku tidak lazim ICT; bagaimanapun, kajian-kajian dalam ruang lingkup sektor awam Malaysia adalah terhad. Oleh itu, kajian ini bertujuan untuk mengenal pasti faktor-faktor signifikan yang mempengaruhi perilaku tidak lazim sebagai input kepada pembentukan dan pengesahan suatu model perilaku tidak lazim ICT dalam ruang lingkup tersebut. Model cadangan ini menyumbang kepada badan ilmu secara teoritikal dengan pemakaian penyelesaian dari pelbagai disiplin seperti faktor etika dari psikologi, faktor keakraban organisasi dari disiplin sosio-kriminologi dan faktor pencegahan umum dari disiplin keselamatan ICT.*

*Kata kunci: Faktor etika, masalah keselamatan ICT, penyelesaian pelbagai disiplin, salah laku ICT, sosio-kriminologi*

## INTRODUCTION

The seriousness of insider ICT abuse is always a major concern to most researchers in this field from as early as the computing days until today (Meyer 1995; Straub and Welke 1998; Stephen 1998; Thompson 1998; Computer Security Institute 2001). As pointed by Breidenbach (2000) quoting Schultz: "Numerically, more attacks come from the outsider now, but …one insider with the right skills can ruin your organisation". Furthermore, the dynamic dispersed of ICT currently have expose employees to encounter more opportunity of unethical situations as compared to those computing days (Cogner et al. 1995; Gattiker and Kelly 1999). Even though appropriate security countermeasures have been in place, the current computing scenario has put ICT abuse to be a continuous problem in most organisation including agencies of the Malaysian Public Sector (MyMIS 2001).

The above justification clearly indicates the inadequacy of the current solution to mitigate ICT abuse. Since ICT abuse behaviour is an intentional act, hence, liked other deviant behavioural studies, the study adopts the Theory of Planned Behaviour (TPB) Model by Ajzen (1985, 1991) as the conceptual framework. TPB model

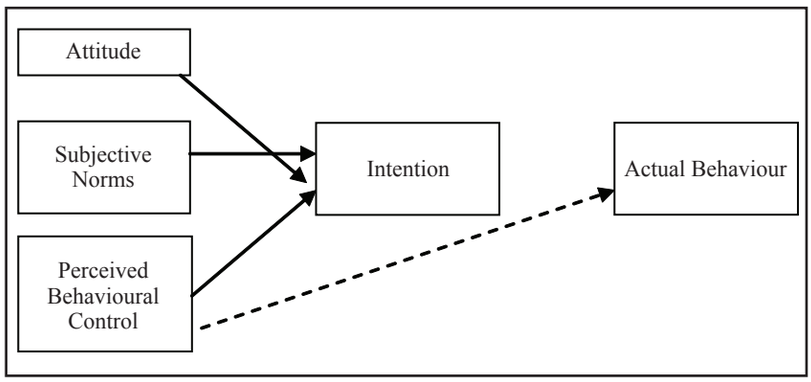


FIGURE 1. Theory of Planned Behaviour

(as depicted in Figure 1) in the past, has successfully predicted abusive behaviour because the theory assumes that intention is a key factor in predicting a person's behaviour.

Based on Figure 1, intentions are formed by the attitude, subjective norms and perceived behavioural control. Whereby (1) attitude is defined as the degree to which the person has a favourable or unfavourable evaluation of the behaviour in question; (2) subjective norms is defined as the influence of social pressure, perceived by the person to perform or not to perform certain behaviour; and (3) perceived behavioural control is defined as the perceived ease or difficulty of performing the behaviour.

Therefore, the current study attempts to explore other factors such as ethical factors and organisational bond factors besides general deterrence factors. The study proposed that the ethical factors based on Information Ethics Theory (IET) can affect attitude, organisational bond factors based on Social Bond Theory (SBT) can affect subjective norms, and general deterrence factors based on General Deterrence Theory (GDT) can affect the perceived behavioural control. (All the above mention theories will be explained in the review of relevant literature section). These factors are integrated into the existing TPB model and assessed the degree to which the new model explained ICT abuse. Based on the above discussions, a conceptual framework was developed as depicted in Figure 2.

## RESEARCH OBJECTIVES AND QUESTIONS

The study seeks to achieve the following objectives:

1. To evaluate the extent of ICT security practice in the Malaysian public sector;
2. To investigate the influence of the ethical factors, organisational bond factors, general deterrence factors on Self Control Intention (SCI), Process Control Intention (PCI) and Technical Control Intention (TCI), respectively;
3. To investigate the influence of the SCI, PCI, TCI on Misfeasors' abuse, Clandestine-users' abuse and Masqueraders' abuse behaviour, respectively;
4. To develop and validate a model for analysing ICT abuse behaviour in the Malaysian Public Sector.

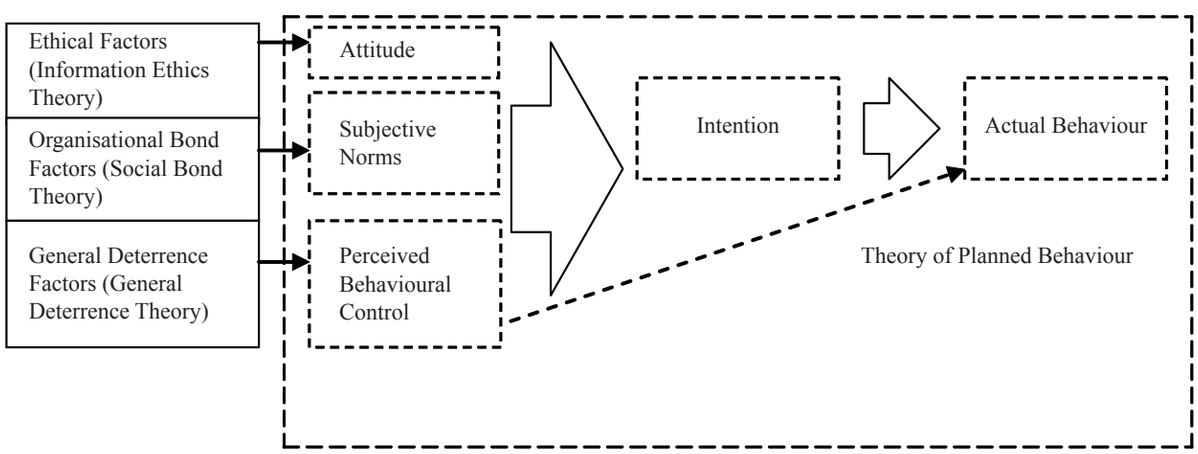


FIGURE 2. Conceptual Framework (based on the Theory of Planned Behaviour)

Hence, the study seeks to answer the following research questions:

1. What is the extent of ICT security practice in the Malaysian Public Sector?
2. Do factors such as ethical, organisational bond and general deterrence, influence the SCI, PCI and TCI, respectively in the Malaysian Public Sector?
3. Do the SCI, PCI, TCI factors influence the frequency of ICT abuse by Misfeasors, Clandestine-users, and Masqueraders, respectively in the Malaysian Public Sector? and
4. Can a model of ICT abuse for the Malaysian Public Sector be developed and validated?

## REVIEW OF RELEVANT LITERATURE

The literature review has identified three gaps in ICT abuse research. The first gap is ICT abuse research mostly focuses solely on the traditional General Deterrence Theory (GDT) which assumes that people make criminal decisions when the expected benefits from the criminal action exceed the costs of punishment (Beccaria 1963). The theory focuses on the security mechanisms such as security policy, security awareness and security systems which aim at increasing the perceived cost of the crime. However, such mechanisms alone failed to significantly reduce ICT abuse. Other solution (Lee and Lee 2002; Lee et al. 2004) is to combine GDT with Social Criminology Theories such as Social Bond Theory by Hirschi (1969) which assumes that all people are naturally inclined to commit crimes unless there exists strong control mechanism or "social bond" such as attachment, commitment, involvement, and beliefs; Social Learning Theory by Akers (1985; 1997) and Akers et al. (1979) which assumes that a person commits a crime because the person has come to associate with delinquent peers; or Social Control Theory by Agnew (1995) which explains negative affect creates pressure for corrective action.

Secondly, many researchers (such as Kowalski 1990; Zalud 1984; Trompeter & Eloff 2002) realise the clamant need for ethical factors in addressing ICT abuse issue but there are limited studies on the combined effects of the ethical theories (such as Information Ethics Theory by Floridi (1999) which formed the seven ethical codes of Institute for Certification of Computer Professional (ICCP), that include the aspect of accountability, conflict of interest, disclosure, personal conduct, protection of privacy, integrity and social responsibility into the existing ICT or computer abuse model (General Deterrence Theory with one or more Social Criminology Theories).

Thirdly, very few empirical studies had looked at ICT abuse behaviour in the public sector setting. Therefore, this study seeks to address these gaps in the hypotheses and research designs generated. Hence, this phenomenon motivates the author to study the factors that could influence the intentions related to ICT abuse behaviour amongst employees in the Malaysian Public Sector. This research aims at developing a model that integrates the factors from the field of ICT security, criminology and ethics, targeted at improving individual ICT practice to act in an ethical responsible way which could significantly reduce the ICT security breaches.

## RESEARCH MODEL

The research model (Figure 3) and its hypothesized relationship was developed based on the findings obtained from the theoretical study conducted within the scope of the conceptual framework (Figure 2). The constructs and variables of the research model are as follows:

1. The construct of "ethical factors" is defined in terms of ethical belief and ethical behaviour that aim to improve the attitude towards the deviant behaviour. 'Ethical belief' is defined as the degree to which an act is belief to be ethical or otherwise. 'Ethical behaviour' is defined as the degree to pursue or not to pursue an action. In both instances actions were based of ICCP's seven ethical code;
2. The "organisational bond factor" construct is defined in terms of attachment, commitment, involvement, and beliefs. The item "attachment" measures the affection and respect that an individual has for others. "Commitment" item measures the person's actual or anticipated investment, reputation, achievements and aspirations in conventional society. "Involvement" item refers to the amount of time and effort spent engaged in informal activities that reinforce employee relationship. The item "beliefs" pertain to the perception towards the moral validity of the law that formed the moral element of the bond;
3. "General Deterrence Factors" construct is defined in terms of the security policy, security awareness and security systems. These security mechanisms were proposed to increase the perceived cost of the crime which then increases the costs of punishment that eventually will decrease the benefits of criminal action. Therefore ICT abuse could be reduced. "Security policy" measures the severity of the policy and it's helpfulness in deterring ICT abuse. "Security awareness" refers to the frequency of deploying, level of awareness amongst employees and the helpfulness of such programme. "Security system" measures the perceived effectiveness of the security system, willingness to invest in procuring the security products or solution and sufficiency of budget allocated;
5. Since this study adopts theory of planned behaviour, "intention" as the key factor in predicting actual behaviour has been employed in this study. The

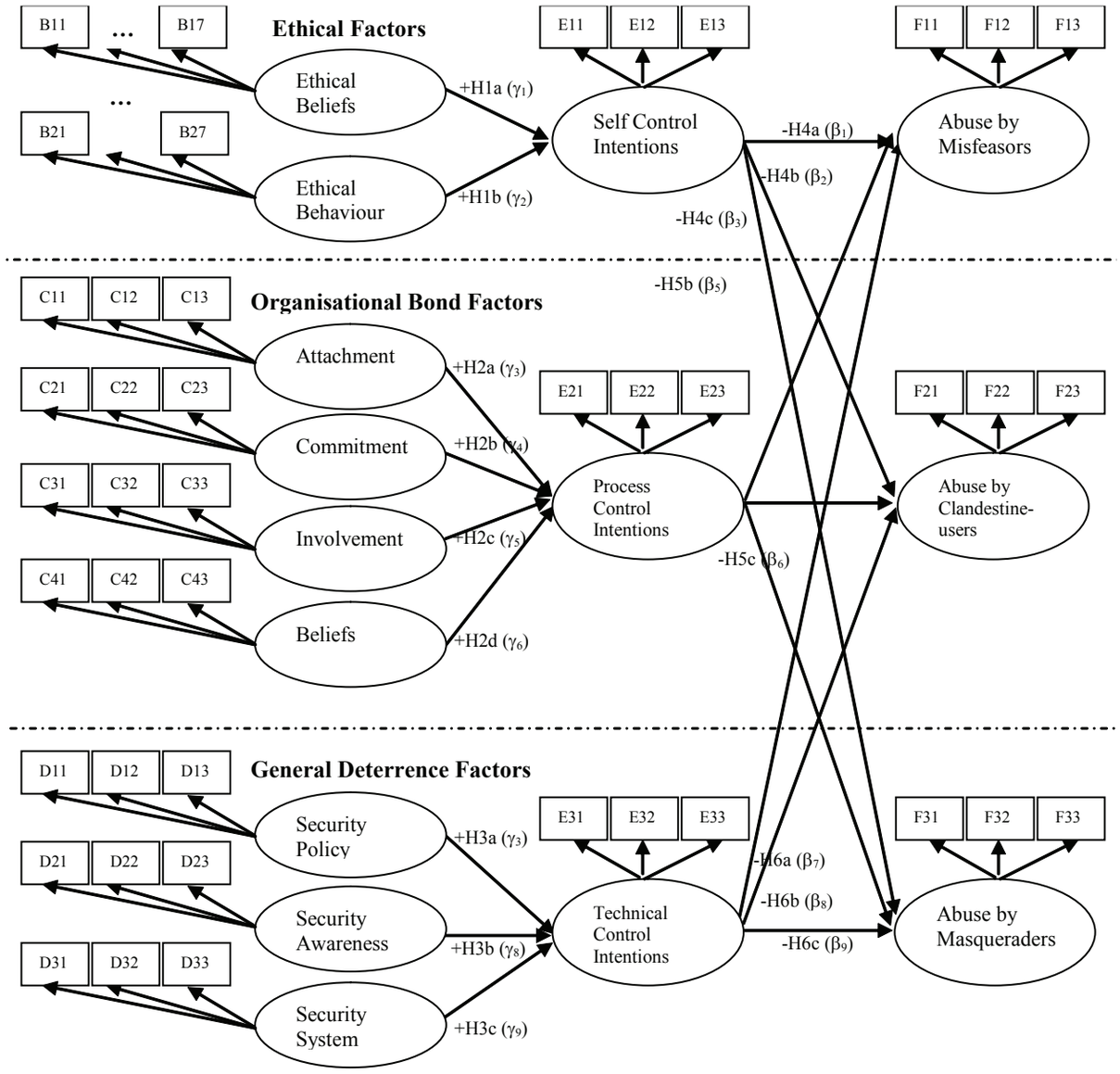


FIGURE 3. Research Model (Measurement Model)

TABLE 1. Concepts, Constructs and Measures of the Research Model

| Concept | Construct | Variables Labels | Measure Description |
|---|---|---|---|
| Ethical Factors (Derived from ICCP code of ethics based on Information Ethics Theory) | Ethical Beliefs | B11 | Do not misuse authority entrusted to me |
| | | B12 | Act faithfully on behalf of employers at all times |
| | | B13 | Do not divulge confidential information to third party |
| | | B14 | Do not use or take credit for work of others |
| | | B15 | Do not exploit the weakness of a computer system for personal gain |
| | | B16 | Do not use confidential information in any unauthorised manner |
| | | B17 | Do not withhold or misrepresent information that is germane to a problem of public concern |
| | Ethical Behaviour | B21 | Accept full responsibility for work that I perform |
| | | B22 | Avoid conflict of interest and insure that employers are aware |
| | | B23 | Do not use the employers' resources for personal gain |
| | | B24 | To act with integrity or honesty at all times |
| | | B25 | Endeavour to share my special knowledge |

| | | | |
|---|---|---|---|
| | | B26 | Protect the privacy and confidentiality of all information entrusted |
| | | B27 | To be socially responsible in the use and dissemination of information |
| Organizational Bond Factors (Derived from Social Bond Theory) | Attachment | C11 | Conversation with co-workers who are in close relationships |
| | | C12 | Communication with co-workers in the same project |
| | | C13 | Respects for co-workers' view and opinions |
| | Commitment | C21 | Desire to succeed within the same unit |
| | | C22 | Importance for the success of your unit |
| | | C23 | Spending time to succeed in the same unit |
| | Involvement | C31 | Chances to participate in informal meetings |
| | | C32 | Personal relationships with many people |
| | | C33 | Willingness to joint in any informal activities |
| | Beliefs | C41 | No matter how small the crime, breaking the law is a serious matter |
| | | C42 | It is wrong when I break the law |
| | | C43 | It is wrong to get around the law even if I can get away with it |
| General Deterrence Factors (Derived from General Deterrence Theory) | Security Policy | D11 | Degree of knowledge of security policy |
| | | D12 | Severity of security policy |
| | | D13 | Helpfulness of security policy |
| | Security Awareness | D21 | Frequency of awareness programmes per year |
| | | D22 | Degree of security awareness |
| | | D23 | Helpfulness of security awareness |
| | Security System | D31 | Degree of security system effectiveness |
| | | D32 | Investment on security system |
| | | D33 | Sufficiency of budget for security system |
| Control Intentions | Self Control Intention | E11 | Restrain from abusing the office Internet access privileges |
| | | E12 | Restrain from opening an ambiguous email with alluring subject |
| | | E13 | Restrain from modifying classified government information/data |
| | Process Control Intention | E21 | Review periodically the processes involving ICT resources |
| | | E22 | Sending out reminders that reinforce security concepts |
| | | E23 | Comply with the agency's ICT security policy |
| | Technical Control Intention | E31 | Ensure that suitable virus defense software is installed |
| | | E32 | Ensure that a monitoring system to identify unauthorised entry |
| | | E33 | Ensure that a properly configured firewall is installed |
| ICT Abuse Behaviours (Derived from Anderson's Perpetrators Matrix) | Misfeasors' Abuse | F11 | Frequency of knowing any individual stealing hardware or software |
| | | F12 | Frequency of knowing any individual abusing Internet access privileges |
| | | F13 | Frequency of knowing any individual using unauthorised software |
| | Clandestine-users' Abuse | F21 | Frequency of unauthorised access |
| | | F22 | Frequency of email services becomes unavailable |
| | | F23 | Frequency of ICT related services in the office becomes unavailable |
| | Masqueraders' Abuse | F31 | Frequency of virus attack incident |
| | | F32 | Frequency of web defacement incident |
| | | F33 | Frequency of IP spoofing incident |

study proposes three intentions which were derived from the three fundamental security countermeasures (Dhillon & Moores 2001) known as informal controls, formal controls and technical controls. Hence, the "Control Intention Factors" construct consist of self control intention derived from informal controls, process control intention refers to formal control and technical control intention derived from technical control. The ultimate aim is to achieve the right balance between various kinds of controls that would be a cost-effective ways to make both accidental and intentional misconduct difficult.

5. The three quantitative items used to measure ICT abuse were: (i) the frequency of ICT abuse by "Misfeasors" including employees and managers, such as hardware loss, abusing Internet privileges and installing unauthorised software; (ii) the frequency of ICT abuse by "Clandestine-users" including employees, managers, vendors, contractors, consultants and outsiders, such as unauthorised access, email spamming and denial of

service attack; and (iii) the frequency of ICT abuse by "Masqueraders" including vendors, contractors, consultants and outsiders, such as virus attack, web defacement and IP spoofing. All of the perpetrators' terms are derived from the Anderson Perpetrators' Matrix (1980) and Lister (1995).

Table 1 shows the concepts, construct and measures of ethical factors, organisational bond factors, general deterrence factors, self control intention, process control intention, technical control intention, Misfeasors' abuse, Clandestine-users' abuse and Masqueraders' abuse. Previous studies (Agnew & White 1992; Elis & Simpson 1995; Makkai & Braithwaite 1994; Paternoster & Mazerolle 1994; Straub & Goodhue 1991; Straub & Welke 1998; Lee & Lee 2001; Lee et al. 2004) have identified that each factor have either independent or a joint effect on the reduction of ICT abuse. However, empirical study has revealed otherwise.

## RESEARCH HYPOTHESES

The study adopted TPB to test the following hypotheses:

H1: Employees with high degree of ethical factors will show positive and significant increase of Self Control Intention (SCI) related to ICT abuse behaviour.

H2: Employees with strong bond factors within organisation will show positive and significant increase of Process Control Intention (PCI) related to ICT abuse behaviour.

H3: Employees with high degree of general deterrence factors will show positive and significant increase of Technical Control Intention (TCI) related to ICT abuse behaviour.

H4: Employees with high degree of control intentions factors to protect ICT asset will reduce the frequency of ICT abuse by Misfeasors.

H5: Employees with high degree of control intentions factors to protect ICT asset will reduce the frequency of ICT abuse by Clandestine-users.

H6: Employees with high degree of control intentions factors to protect ICT asset will reduce the frequency of ICT abuse by Masqueraders.

This study utilized a 7-point Likert-type scale for measuring variables. To summarize data and develop constructs, the author used the path analysis approach. Maximum likelihood estimation was used in the measurement and structural models. This analysis provided a simultaneous test of the model relationships as well as estimates for measurement error.

For the pilot study, the survey questionnaire were distributed to 50 employees who are users, system developers, system administrators, system managers, middle level managers and ICT division directors or deputy directors mostly located in Putrajaya. The return rate was 91%. On the basis of the pilot study results, a new questionnaire was developed in two languages, English and Bahasa Malaysia. The self-administered questionnaires were distributed to 600 employees from 13 pilot agencies of the E-government projects, 214 questionnaires were returned making the response rate of 35.7%, 12 questionnaires were discarded because of missing items. The electronic government agencies were chosen based on the high profile electronic government application which are highly dependent on ICT resources in critical and sensitive agencies or lead agencies in electronic government projects.

The study chose a natural setting approach in which the participants have to evaluate the ICT abuse behaviour based on the ICT security practice at work or if no security initiatives in place, used their perception. The study applied a purposive sampling technique and within the sample a stratified techniques was applied to ensure that the respondents were well represented by various departmental, organisational and job levels.

## DEMOGRAPHIC PROFILE OF THE SAMPLE

Table 1 presents personal characteristics, professional characteristics, ICT security practice, and reasons for abuse of 214 respondents. In terms of personal characteristics, the survey were mostly participated by female respondents (62.6%). The majority of the respondents (28.5%) were from the age group of '30-34'. Most of the sample acquired diploma (41.6%) as their highest level of education. Majority of them had average level of ICT proficiency (39.3%). In terms of professional characteristics, the questionnaires were responded by mostly from operating agencies (64.5%). Database administrators (28.0%) were the largest group of position level participated. Most of the subjects have service the government at least 11-15 years (35.5%). The findings indicate that the respondents were matured, educated, had average ICT proficiency, involved with handling of ICT resources (operating agency) and had sufficient years of servicing the government which formed an appropriate foundation for subject of analysis.

## ICT SECURITY PRACTICE IN THE MALAYSIAN PUBLIC SECTOR

Table 2, presents the ICT security practice within the Malaysian Public Sector as perceived or based on natural setting of the respondents. The purpose of results obtained is to answer the first research question which is to evaluate the extent of ICT security practice

TABLE 2. Demographic Profile of the Sample

| Personal Characteristic | Characteristic | Item | Frequency | Percent |
|---|---|---|---|---|
| | Gender | Male | 80 | 37.4 |
| | | Female | 134 | 62.6 |
| | Age | Below 24 | 5 | 2.3 |
| | | 25-29 | 42 | 19.6 |
| | | 30-34 | 61 | 28.5 |
| | | 35-39 | 32 | 15.0 |
| | | 40-44 | 43 | 20.1 |
| | | 45-49 | 21 | 9.8 |
| | | Above 50 | 10 | 4.7 |
| | Education | SPM | 28 | 13.1 |
| | | Diploma | 89 | 41.6 |
| | | Bachelor | 73 | 34.1 |
| | | Masters | 20 | 9.3 |
| | | Doctorate | 4 | 1.9 |
| | ICT Proficiency | Below-average | 43 | 20.1 |
| | | Average | 84 | 39.3 |
| | | Above-average | 59 | 27.6 |
| | | Power-users | 28 | 13.1 |
| Professional Characteristics | Agency Type | Operating Agency | 138 | 64.5 |
| | | Central Agency | 76 | 35.5 |
| | Position level | Managers | 58 | 27.1 |
| | | Database Admin. | 60 | 28.0 |
| | | Deputy Director | 15 | 7.0 |
| | | Programmer | 58 | 27.1 |
| | | Principal Asst. Dir. | 23 | 10.7 |
| | Years of Service | Less than 1 year | 5 | 2.3 |
| | | 1 - 5 years | 40 | 18.7 |
| | | 6 - 10 years | 50 | 23.4 |
| | | 11 - 15 years | 76 | 35.5 |
| | | 16 - 20 years | 26 | 12.1 |
| | | More than 21 years | 17 | 7.9 |

in the Malaysian Public Sector. In terms of ICT security initiatives, only 39.7% had written security policy in their organisation. The result indicates that written security policy had not been developed in most of the organisation. This could due to many reasons but the most common reason is because most organisations lack of knowledgeable manpower in ICT security to develop the security policy. Most of the employees state that their organisation had deployed smartcards (68.2%) as an effort to secure their ICT resources. Finally, the survey reveal that respondent perceived the most common reason for ICT abuse is "ignorance of ICT security knowledge" which is about 73.8% and 61.2% perceived reason for abusing ICT resources is because of "desire for personal gains".

## VALIDITY AND RELIABILITY OF THE RESEARCH MODEL

Both validity and reliability analysis was performed using SPSS 14.0. With regard to the construct validity, Table 4, Table 5 and Table 6 shows the factor analysis performed on the independent, moderating and dependent variables. As suggested by Hair et al. (2006), since the sample size is in the range of 200 to 250, the acceptable loading factor is 0.4. Hence, the construct validity reveals that all the factors were loaded more than 0.4, indicating the validity of the construct.

The result of the reliability analysis is as shown in Table 7. The result for the entire construct was found to be at alpha Cronbach greater than 0.7, and the value is acceptable as suggested by many social science studies. Hence, the result indicates that the constructs used in the study is reliable.

TABLE 3. ICT Security Practice in the Malaysian Public Sector

| Characteristics | Items | Frequency | Percent |
|---|---|---|---|
| ICT Security Initiatives | Had Security Policy | 85 | 39.7 |
| | Had Security Awareness | 58 | 27.1 |
| | Use ethical codes in handling ICT resources | 37 | 17.3 |
| | Performed risk assessment | 64 | 29.9 |
| Deployment of ICT Security Counter measure | Firewalls | 102 | 47.7 |
| | Anti-virus Software | 109 | 50.9 |
| | Passwords | 101 | 47.2 |
| | Biometric-based | 39 | 18.2 |
| | Smart cards | 146 | 68.2 |
| | Tokens | 57 | 26.6 |
| | Disk Drive Locks | 105 | 49.1 |
| | Badges | 110 | 51.4 |
| | Electronic locks | 57 | 26.6 |
| | Encryption | 107 | 50.0 |
| | Intrusion Detection System | 83 | 38.8 |
| | None | | |
| Reason for Abuse | Ignorance of proper professional conduct | 130 | 60.7 |
| | Revenge on the organisation | 54 | 25.2 |
| | Desire for personal gains | 131 | 61.2 |
| | Ignorance of ICT security knowledge | 158 | 73.8 |
| | Misguided playfulness | 80 | 37.4 |
| | Not knowing the consequence of such act | 127 | 59.3 |
| | Negligence | 121 | 56.5 |
| | Poor ICT security countermeasures | 117 | 54.7 |

TABLE 4. Factors on the Independent Variables – Rotated Factor Matrix

| Items | Factor | | |
|---|---|---|---|
| | 1 | 2 | 3 |
| Ethical Factors | | | |
| Highly Accountable | .938 | .092 | .029 |
| No Conflict of Interest | .872 | .075 | .003 |
| No Information Disclosure | .948 | .107 | .054 |
| Proper Personal Conduct | .921 | .094 | .023 |
| Protects Privacy | .913 | .036 | .008 |
| Ensure Integrity | .957 | .108 | .035 |
| No misrepresenting information | .949 | .131 | .020 |
| Accepting Responsibility | .948 | .102 | .039 |
| Avoiding Conflict | .832 | .087 | .000 |
| No abuse of employer's resources | .930 | .135 | .073 |
| Act with honesty | .905 | .134 | .034 |
| Sharing knowledge | .897 | .082 | -.029 |
| Protecting confidentiality | .939 | .120 | .058 |
| Socially Responsible | .938 | .124 | .063 |
| Organisational Bond Factors | | | |
| Knowledge pertains to Security Policy | .030 | .211 | .914 |
| Severity of Security Policy | .018 | .263 | .933 |
| Helpfulness of Security Policy | .013 | .255 | .908 |
| Frequent Awareness Programmes | .044 | .236 | .932 |
| High Awareness Level | .041 | .283 | .944 |
| Helpfulness of Awareness Programmes | .014 | .265 | .944 |
| Effectiveness of Security System | .045 | .223 | .936 |
| Investment on Security System | .045 | .234 | .942 |
| Budget Allocation for Security System | .023 | .217 | .942 |

| | | | |
|---|---|---|---|
| General Deterrence Factors | | | |
| Close with Co-workers | .111 | .852 | .174 |
| Communicate with all Co-workers | .130 | .929 | .230 |
| Respect Co-workers' Opinion | .108 | .917 | .215 |
| Desire to Succeed | .078 | .935 | .173 |
| Importance of Success | .097 | .943 | .192 |
| Work Hard for Success | .150 | .904 | .269 |
| Volunteer to Participate Informal Meetings | .088 | .942 | .146 |
| Secretariat to Informal Activities | .125 | .927 | .234 |
| Willingness to Joint Any Informal Activities | .130 | .837 | .241 |
| Beliefs that Crime is a Serious Matter | .114 | .925 | .226 |
| Beliefs that Breaking the Law is Wrong | .118 | .930 | .215 |
| Beliefs that Obeying the Law is Crucial | .142 | .873 | .269 |

TABLE 5. Factors on the Moderating Variables – Rotated Factor Matrix

| Items | Factor | | |
|---|---|---|---|
| | 1 | 2 | 3 |
| Self Control Intention | | | |
| Periodic Review of Processes | .139 | .678 | .187 |
| Send out Reminders | .151 | .928 | .294 |
| Comply to Security Policy | .175 | .749 | .338 |
| Process Control Intention | | | |
| Restrain from Abusing Internet Access Privileges | .964 | .173 | .157 |
| Restrain from Opening Ambiguous Email | .973 | .170 | .151 |
| Restrain from Modifying Government Information | .910 | .146 | .106 |
| Technical Control Intention | | | |
| Install Virus Defense Software | .186 | .349 | .525 |
| Install Intrusion Detection System | .090 | .218 | .963 |
| Install Firewall | .141 | .312 | .716 |

TABLE 6. Factors on the Dependent Variables – Rotated Factor Matrix

| Items | Factor | | |
|---|---|---|---|
| | 1 | 2 | 3 |
| Misfeasors' Abuse | | | |
| Abusing ID privileges | .825 | .127 | .100 |
| Abusing Internet Access Privileges | .912 | .128 | .159 |
| Using Unauthorised Software | .911 | .143 | .140 |
| Clandestine-users' Abuse | | | |
| Virus Attack Incident | .143 | .147 | .736 |
| Defacing Web Site | .142 | .168 | .961 |
| IP Spoofing Incident | .077 | .158 | .605 |
| Masqueraders' Abuse | | | |
| Unauthorised Access | .161 | .831 | .205 |
| Unavailability of Email Services | .104 | .994 | .118 |
| Attack on ICT Related Services | .138 | .740 | .222 |

TABLE 7. Constructs and Reliability Tests

| Construct | Items in Scale | Cronbach Alpha |
|---|---|---|
| Ethical Beliefs | 7 | 0.97 |
| Ethical Behaviour | 7 | 0.97 |
| Attachment | 3 | 0.85 |
| Commitment | 3 | 0.82 |
| Involvement | 3 | 0.85 |
| Beliefs | 3 | 0.69 |
| Security Policy | 3 | 0.73 |
| Security Awareness | 3 | 0.77 |
| Security Systems | 3 | 0.81 |
| Self Control Intention | 3 | 0.98 |
| Process Control Intention | 3 | 0.88 |
| Technical Control Intention | 3 | 0.82 |
| Misfeasors Abuse | 3 | 0.93 |
| Clandestine-users Abuse | 3 | 0.91 |
| Masqueraders Abuse | 3 | 0.82 |

ICT ABUSE (ICTA) MODEL DEVELOPMENT AND VALIDATION

Figure 4 provides the full model that was tested. Bold lines in the figure indicate the significant paths among latent constructs, thin lines represent non-significant paths and the dotted lines show significant paths rejecting the hypotheses. The measures of the overall goodness-of-fit for the entire model are illustrated in Table 8. The computation procedures were using AMOS 6.0, the fitness of the research model was assessed in the results; $\chi^2$ – value = 454.934 ($P$ = 0.000), degree of freedom (d.f.) = 254, $\chi^2$/d.f. = 1.791, GFI = 0.863, AGFI = 0.811, NFI = 0.873, NNFI = 0.921 and RMSEA = 0.061.

When a model is correct but its conditions may be incorrect, the $\chi^2$ – value is likely to appear larger than it should, indicating a problem of fit: the greater the sample size, the lower the $\chi^2$ – value. From this paper's perspective, it is therefore advisable to the $\chi^2$ – value in conjunction with other fitness indices. Medsker et al. (1994), suggested that $\chi^2$/d.f. ratios of less than 5 can be interpreted as indicating a good fit, with ratios less than 2 indicating over fitting. The current ICTA model is reasonable in $\chi^2$/d.f.

The typical null model is an independence model, that is, one in which the observed variables are assumed to be uncorrelated and their counterpart (non-normed fit index, NNFI) should also have a comparably high value. The values of NFI 0.873 means that the relative overall fit of the model is 87% better than that of the null model estimated with the same data. The fitness of the overall model was assumed appropriate, based on high fitness indexes, even though the goodness of the fit index (GFI) and adjusted GFI (AGFI) did not satisfy Gefen et al.'s recommended minimum values of 0.90 and 0.80, respectively (2000).

TABLE 8. Measures of Model Fitness

| Fit Measure | Recommended Value | Fitness Measure |
|---|---|---|
| $\chi^2$ | | 454.934 |
| $\chi^2$/d.f. | < = 3.0 | 1.791 |
| NFI | > = 0.80 | 0.873 |
| NNFI | > = 0.90 | 0.921 |
| GFI | > = 0.90 | 0.863 |
| AGFI | > = 0.80 | 0.811 |
| RMSEA | < = 0.08 | 0.061 |

## FINDINGS

In summary, the various measures of overall model goodness-of-fit and the strength of paths provided sufficient support for it as an acceptable representation of the hypothesised constructs and their relationships. Table 9 summarises the results of the testing of the research hypotheses to address the second and third research questions. Some of these results provide good support for the hypotheses, although the paths from the ethical belief to SCI, commitment and involvement to PCI, security awareness to TCI, PCI and TCI to Misfeasors' abuse, TCI to Clandestine-users' abuse, SCI and PCI to Masqueraders' abuse are not accepted.

The R sq. scores indicated that constructs constituted reasonably predictors of intentions and ICT abuse. Figure 4 presents schematic path analysis.

In order to answer the second research question, the first, second, and third hypotheses were tested. The first hypothesis reveals ethical behaviour factor is the most significant predictor of Self Control Intention ($\gamma_2$ = 0.889***). The second hypothesis testing indicates that attachment and belief factors were both significant in predicting Process Control Intention. However attachment factor appeared to be the top predictor of Process Control Intention with $\gamma_3$ = 0.732***. The third hypothesis testing reveal that security policy factor was the most significant predictor of Technical Control Intention ($\gamma_7$ = 0.762***) amongst the factors of security awareness and security system.

In the effort to answer the third research question, the forth, fifth and sixth hypotheses were tested. The forth hypothesis shows that amongst the control intention factors of Self Control Intention, Process Control Intention and Technical Control Intention, the Self Control Intention factor appeared to be the only significantly predictor of ICT abuse by Misfeasors ($\beta_1$ = -0.782***). This empirical evidence suggests that high self control intention would significantly reduce ICT abuse by Misfeasors or internal users only but not other control intentions. The finding is consistent with the study by Dhillon and Moores (2001), who postulate that only self control intention or the intention to perform informal controls would appropriately influence internal employees because this type of control could develop

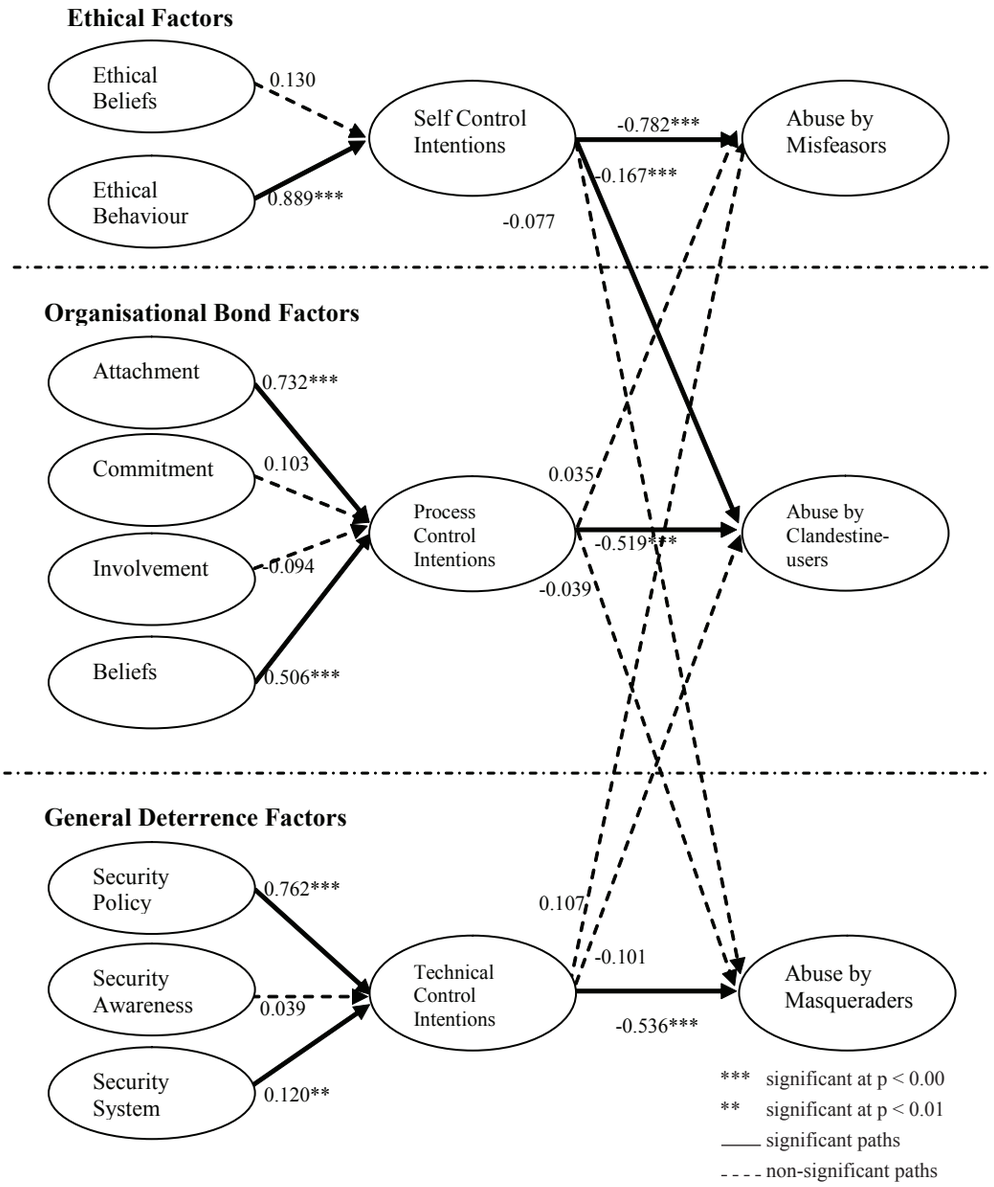


FIGURE 4. ICT Abuse (ICTA)

a sub-culture that enables everyone to understand the importance of appropriate behaviour and attitudes or making the employees believe in the organisation and assuring individual accountability for any misconduct such as abusing office Internet access privileges (visiting pornographic website during office hours or chatting).

The fifth hypothesis reveals that both Self Control Intention and Process Control Intention factors were significant predictors of ICT abuse by Clandestine-users. However, amongst the two factors, Process Control Intention factor was the most significant predictor ($\beta_5$ = -0.519***). These results indicate that the intention to comply with ICT security policy and reinforcing security countermeasures through reminders release by agency's security unit are significantly important to reduce the rate of ICT abuse by Clandestine-users. For the last hypothesis testing, the results indicates that Technical Control Intention is the sole significant predictor of ICT abuse by Masqueraders ($\beta_9$= -0.536***). Even though Self Control Intention factor is not significant to predict Masqueraders' abuse, interestingly, it positively affects Masqueraders' abuse. Which predict that the higher the Technical Control Intention factor the higher the rate of ICT abuse by Misfeasors (insiders). The empirical test reveals that only high technical control intention would significantly reduce the rate of ICT abuse by Masqueraders. This is traditionally true that Masqueraders (outsiders) can be controlled by increasing the level of technical control intention such as the intention to install properly configured firewall systems, intrusion detection systems, anti-

TABLE 9. Results of Hypotheses Testing

| Research Questions | Research Hypotheses | Paths | | R sq. | Standardized paths coefficient | Hypotheses Results |
|---|---|---|---|---|---|---|
| | | From | To | | | |
| RQ2: | H1a | Ethical Belief | Self Control Intention | 0.599 | 0.130 | Rejected |
| | H1b | Ethical Behaviour | | | 0.889 *** | Accepted |
| | H2a | Attachment | Process Control Intention | 0.586 | 0.732 *** | Accepted |
| | H2b | Commitment | | | 0.103 | Rejected |
| | H2c | Involvement | | | -0.094 | Rejected |
| | H2d | Belief | | | 0.506 *** | Accepted |
| | H3a | Security Policy | Technical Control Intention | 0.481 | 0.762 *** | Accepted |
| | H3b | Security Awareness | | | 0.039 | Rejected |
| | H3c | Security Systems | | | 0.120 ** | Accepted |
| RQ3: | H4a | Self Control Intention | Misfeasors' Abuse | 0.572 | -0.782 *** | Accepted |
| | H4b | Process Control Intention | | | 0.035 | Rejected |
| | H4c | Technical Control Intention | | | 0.107 | Rejected |
| | H5a | Self Control Intention | Clandestine-users' Abuse | 0.550 | -0.167 *** | Accepted |
| | H5b | Process Control Intention | | | -0.519 *** | Accepted |
| | H5c | Technical Control Intention | | | -0.101 | Rejected |
| | H6a | Self Control Intention | Masqueraders' Abuse | 0.542 | -0.077 | Rejected |
| | H6b | Process Control Intention | | | -0.039 | Rejected |
| | H6c | Technical Control Intention | | | -0.536 *** | Accepted |

*** $p < 0.001$ **$p < 0.01$ *$p < 0.05$

RQ2 : Do factors such as ethical, organisational bond and general deterrence, influence the level of SCI, PCI and TCI in the Malaysian Public Sector?
RQ3 : Do SCI, PCI, TCI influence the frequency of ICT abuse by Misfeasors, Clandestine-users, and Masqueraders in the Malaysian Public Sector?

virus systems and other security initiatives such as severity of security policy were sufficient to reduce ICT abuse by Misfeasors.

## CONCLUSION

The main motivation for this study was to propose Information Ethics Theory and Social Bond Theory into ICT abuse research because most previous studies have analysed ICT/computer abuse relying solely on general deterrence theory. In this study, we empirically investigated the application of Information Ethics Theory, Social Bond Theory and General Deterrence Theory in the Theory of Planned Behaviour model's perspective. The research model drew the introduction of several new factors. These were (a) ethical factors (derived from Information Ethics Theory) – ethical belief and ethical behaviour pertaining to ethical codes namely accountability, protection of privacy, integrity, avoid conflict of interest, disclosure, and personal conduct; (b) organisational bond factors derived from Social Bond Theory, namely, attachment, commitment, involvement and belief; (c) control intention factors, namely, self control intention, process control intention and technical control intention; and (d) ICT abuse behaviours, namely, misfeasors, clandestine-users and masqueraders. A new ICT abuse model was developed and validated through the process of Structural Equation Modeling which involved the utilisation of SPSS 14 and AMOS 6. This research suggested that the education/training of ethical conduct in handling ICT resources, reinforcement of social bond through organisational bond, and intention to apply a more balanced effort in security countermeasures were another mechanism that could help reduce ICT abuse in organisations.

As with all survey-type studies, the interpretation of the results should make allowances for sampling constraints. One limitation is that the sample, agencies of the e-government projects of the Malaysian public sector may not be representative of all ICT users in the government. Another probable limitation is that the study might not have included all factors necessary to analysing ICT abuse, such as culture, environment, religion, stakeholder or other human characteristics.

## REFERRENCES

Agnew, R. 1995. Testing the leading crime theories: an alternative strategy focusing on motivational processes. *Journal of Research in Crime and Delinquency* 30(4): 363-398.

Ajzen, I. 1985. From intentions to actions: a theory of planned behaviour. In *Action control: from cognition to behaviour*, edited by Kuhl J., Beckman, J. New York: Springer-Verlag.

Ajzen, I. 1991. The theory of planned behaviour. *Organisational Behaviour and Human Decision Processes* 50(2): 179-211.

Akers, R.L. 1985. *Deviant Behaviour: A Social Learning Approach*. Belmont: Wadsworth.

Akers, R.L. 1997. *Criminological Theories: Introduction and Evaluation*. 2nd edition. Los Angeles: Roxbury Publishing.

Anderson, J.P. 1980. *Computer Security Threat Monitoring and Surveillance*. Fort Washington, PA: James P. Anderson Co.

Beccaria, C. 1963. On crime and punishments. *Journal of Information & Management* 41: 707-718.

Breidenbach, S. 2000. How secure are you? *Information Week* 8: 71-78.

Computer Security Institute. 2001. Issues and trends: 2001 CSI/FBI Computer abuse and security survey, CSI, San Francisco, CA.

Conger, S., Loch, K.D. & Helft, B.L. 1995. Ethics and information technology use: a factor analysis of attitudes to computer use. *Information Systems Journal* 5: 161-84.

Dhillon, G. & Moores, S. 2001. Computer crimes: theorizing about the enemy within. *Computer & Security* 20(8): 715-723.

Floridi, L. 1999. Information ethics: On the philosophical foundation of computer ethics. *Ethics and Information Technology* 1(1): 37-56.

Gattiker, U.E. & Kelly, H. 1999. Morality and computers: attitudes and differences in moral judgments. *Information Systems Research* 10(3): 233-54.

Hirschi, T.A. 1969. *Causes of Delinquency*. Berkeley: University of California Press.

Kowalski, S. 1990. Computer ethics and computer abuse: a longitudinal study of Swedish University students. IFIP TCII 6th International Conference on Information Systems Security.

Lee, J. & Lee, Y. 2002. A holistic model of computer abuse within organisations. *Information Management & Computer Security* 10(2): 57-63.

Lee, S., Yoo, S. & Nah, F. 2004. An integrated model based on social control and general deterrence theories. *Journal of Information & Management* 41: 707-718.

Lister, J.J. 1995. Intrusion detection systems: an introduction to the detection and prevention of computer abuse. Thesis, University of Wollongong.

Malaysian Public Sector Management of ICT Security Handbook (MyMIS). 2002. Kuala Lumpur: Government Printers.

Meyer, J. 1995. From the editor. *Computer & Security* 14(1): 2-3.

Stephen, H. 1998. Recent security surveys. *Computer & Security* 17(3): 207-10.

Straub, D.W. Jr. & Welke, R.J. 1998. Coping with systems risk: security planning models for management decision making. *MIS Quarterly* 22(4): 441-65.

Thompson, D. 1998. 1997 computer abuse and security survey. *Information Management & Computer Security* 6(2): 78-101.

Trompeter, C.M. & Eloff, J.H.P. 2002. A framework for the implementation of socio-ethical controls in information security. *Computer & Security* 20: 384-391.

Zalud, B. 1984. IBM Chief urges DP education, social responsibility. *Data Management* 22(9): 30-74.

Safiah Sakri
Juhana Salim
Tengku Mohammed Tengku Sembok
Fakulti Teknologi dan Sains Maklumat
Universiti Kebangsaan Malaysia
43600 Bangi, Selangor Darul Ehsan. Malaysia
Email: js@ftsm.ukm.my; tmts@ftsm.ukm.my