Organizational Climate and Individual Factors Effects on Information Security Compliance Behaviour

Noor Ismawati Jaafar
Adnan Ajis

Department of Operations and MIS
Faculty of Business and Accountancy
University of Malaya
50603 Kuala Lumpur, Malaysia.

Abstract

This study examines the organizational and individual factors that affect the information security compliance behaviour (ISCB) in a secured organization. A survey was conducted among 400 military personnel. A questionnaire was used to collect data on ISCB and the organizational climate and individual factors namely upper management practices, direct supervisory practices, co-worker socialization, self-efficacy, IS perception and personal innovativeness. As a result of this study, four factors affect ISCB. One factor is an organizational and the remaining are individual factors. These are co-worker socialization (CWS), information security perception (ISP), computer self-efficacy (CSE) and personal innovativeness (PI). It is found that ISP is the strongest determinant of ISCB. Detailed information security (IS) planning and a programme should be implemented by top management in the organization. Despite the different roles and responsibilities that come with different levels in the organization, all these users use information systems or the information it produces. This study provides evidence on how the social cognitive theory is combined with organizational and individual factors to study information security compliance in a secured organization.

Keywords: Information security behaviour, organizational climate, information security perception, computer self-efficacy, personal innovativeness

Introduction

Information is now exposed to a growing number and a wider variety of threats and vulnerabilities. Whatever methods are used to obtain the information or means by which it is shared or stored, it should always be appropriately protected. In addition to the threats and vulnerabilities, the growing connection of computers has opened up new challenges to the security of information. In addition, the internal threat is also an issue that should be emphasized in information systems, as it can also contribute to the negative impact on an organization's information security. Normally, the external threat tends to be easier to detect compared to internal threat. According to Colwill (2010), internal threats, such as a malicious insider, have the capability of contributing more damage to the organization compared to an outside attacker. Insider threats have many opportunities and advantages in accessing valuable assets of the organization. They have knowledge of how to gather valuable information easily and know how to cover their actions. Unfortunately, most organizations emphasize external threats rather than internal threats. According to McCue (2008), many organizations emphasize less on control and protection from insider threats. They focus more on external threats, with 90% of security controls and monitoring only for external threats. In his research, it was found that 70% of fraud is perpetrated by insiders rather than external threats.

Many organizations are moving towards information technology by using many computer networks. Employees are accessing the Internet, especially on social networking sites like Facebook or Friendster. They have posted personal information related to their jobs to these web sites without taking into consideration IS matters. Sometimes the computers that they use have connections to the Internet, and may contain restricted data or confidential information. Anybody from outside can access all the data in the computers over the Internet without permission or being discovered.

In view of the importance and confidentiality of information, this study is being conducted to examine the general information security compliance behaviour (ISCB). Therefore, the study will focus on addressing the question of "What are the organizational climate and individual factors that affect the level of IS Compliance Behaviour (ISCB)?"

Background of Study

IS Compliance Behaviour (ISCB)

Griffin and Neal (2000) defined ISCB as the set of core IS activities that need to be carried out by individuals to maintain information security. As a response to Griffin and Neal's (2000) definition above, Chan et al. (2005) in their study stated that in order to make a recommended (compliant) behaviour, an employee needs the skills to perform the required actions and is also influenced by a conducive information security climate. For this study, we will use Griffin and Neal's (2000) definition as the main reference. Mathisen (2004) regarded ISCB to be the understanding of the importance of information security and the display of appropriate behaviour. Raising the state of awareness leads to better attitudes and behaviour regarding IS; which is a change that refers to the individual level. He selects a number of metrics for awareness that represent "good" security behaviour, for example, the number of reported security incidents or number of hits to security Web pages.

Aytes and Connolly (2003) introduced a model of user behaviour that emphasizes factors related to user perception of risk and choices based on that perception. In this model, sources of information, such as friends, policies, procedures and personal experiences, provide information that contributes to the knowledge of users. Here, the knowledge of users refers to threats, vulnerabilities and measures to raise awareness against the potential consequences to themselves or other sand the cost of secure behaviour.Pahnila, Siponen and Mahmood (2007) studied employees' behaviour towards information system security policy compliance. They introduced the central factors of their model, which are attitude towards compliance, intention to comply and actual compliance with information system security policies. They are based on the widely used and accepted Theory of Reasoned Action (TRA). Attitude indicates a person's positive or negative feelings towards some stimulus object.

Chan et al. (2005) in their study found that employee's compliant behaviour is positively impacted by their perception of the IS climate and self-efficacy. This result indicates that compliant behaviour is dependent on a combination of organizational and personal factors. However, the two antecedents explained 26.5% of the variance in compliant behaviour. Therefore, additional antecedents need to be included to increase explanatory power. Brady (2011), in his study, agreed that more attention needs to be given to the social and behavioural aspects of information security in academic medical centres. Security behaviour has been determined to be a key factor affecting health care organizations' security effectiveness and security compliance.

Social Cognitive Theory (SCT)

According to Bandura (1989), SCT promotes a model of causation involving triadic reciprocal determinism. This theory explains the relationship between behaviour, environmental and individual factors. All three factors are interrelated and influence each other bi-directionally. He also explained that "reciprocal causation does not mean that the different sources of influence are of equal strength. Some may be stronger than others nor do the reciprocal influences all occur simultaneously". According to Bandura (1997), the SCT is how humans achieve and sustain particular behavioural patterns and also create the foundation for intervention strategies. It explains that assessment of changes in behaviour depends on environmental, human and behavioural factors. The SCT can be used as a framework for development, implementation and assessment programmes. According to Parraga (1990), environmental refers to factors that can influence human behaviour, such as the social and physical environment. As he mentioned, social environment includes family, friends and colleagues, while physical environment refers to the size of a room, the temperature or the availability of certain foods. He also explains that the framework for understanding behaviour can be provided through the environment and situation. When discussing the situation, it can refer to the cognitive or mental environment that may affect a human's behaviour. According to Glanz et al. (2002) the situation shows the human perception of the place, time, physical characteristics and activity.

As the SCT stated, the three factors of environment, people and behaviour constantly influence each other. Glanz et al. (2002), explained that "Behaviour is not simply the result of the environment and the person, just as the environment is not simply the result of the person and behaviour".

As discussed, the environment can produce the behaviour model. Therefore, according to Bandura (1997), "*Observational learning* occurs when a person watches the actions of another person and the reinforcements that the person receives". Meanwhile, the behaviour concept can be viewed in different ways. Behavioural capability means that if a person is to perform behaviour he must know what the behaviour is and have the skills to perform it.

Factors That Affect IS Compliance Behaviour (ISCB)

Organizational Climate

Organizational climate is defined as "a set of attributes specific to a particular organization that may be induced from the way the organization deals with its members and its environment" (Campbell et al., 1970). It is as perceptual as well as an individual attribute. Climate in this approach is viewed as a summary or global perception held by individuals about their organisational environment. In this study organization climate is one of the independent variables. There are three factors in these variables, namely, Upper Management Practice (UMP), Direct Supervisory Practice (DSP) and Co-worker Socialization (CWS).

Upper Management Practice (UMP)

Management support for IS is required in the Malaysian Army. Top management support is a key recurrent factor critical for the implementation of effective information systems. Many previous studies have been done to show that management support has a pivotal impact on information systems' implementation success. According to Chan et al. (2005), the practices by upper management are mostly based on the customary actions of management as observed by the individual employee. They also found in their study a correlation between UMP and employee's perception of the information security climate and also between employee's perceptions and ISCB. Decker (2008) considered management factors in his study and found a positive correlation between the management factors and the end users' perceptions of their security awareness level. Here IS level refers to understanding the role in protecting information, protecting passwords, keeping a backup of important information, and generally reporting a higher commitment to the security mission of the organization. Before that, previous researchers like Murray (1991) stated that most companies management implement good information security technically (e.g., power supply backup), but often forget to emphasize the awareness of information security to their staff and provide them with information system security instructions to follow. Consequently, most information system security problems are caused by employees who do not appreciate the risks inherent in their actions. Straub (1990) studied whether the decision of organization management to invest in security systems will reduce criminal misuse of computers. He suggested that publicly known efforts to detect abuse may significantly deter abusive behaviour. He also suggested information system security officers to conduct some action to be taken as follows: First, establish the information systems users' policy. Second, is to inform and train information system users about acceptable system use. Third, is to strengthen information system security efforts (e.g., assigning and monitoring passwords) and fourth, to consider the implementation of software preventives (e.g., RACF, Top Secret).Thus, hypothesis 1in this study is as follows:

H1:*UMP has a positive effect on ISCB.*

Direct Supervisory Practices (DSP)

According to Chan et al. (2005), direct supervisory practices refer to the repeated actions of direct supervisors as observed by the individual employee. In this study, supervisors refer to Army officers or senior ranks and also immediate commanders for any soldiers. Normally officers or senior rank official agents of the organization have the most frequent interaction with their subordinates or soldiers. They are the most qualified icons that can influence their soldiers, and, hence, capable of achieving the goals of the unit or organization. The study found a positive relationship between direct supervisory practices and ISCB. This finding suggests that a strong IS climate can be created by engaging all levels of the organization, i.e., top management, middle management (intermediate supervisors), and junior employees. Zohar and Luria (2003), in their study, found that there is a relationship between supervisory practices and employee's perception of safety climate. Furthermore, to support this study, Chan et al. (2005) gave an example those employees who observe their supervisors as giving greater emphasis to performance over the observance of prescribed safety procedures. Thus, we hypothesize the second hypothesis as follows:

H2:*DSP has a positive effect on ISCB.*

Co-Worker Socialization (CWS)

Put simply, co-workers are people who share a workplace with each other. The study of co-worker dynamics has absorbed many psychologists, since relationships between co-workers can be quite interesting and very complex. According to Chan et al. (2005), co-worker socialization refers to the daily interactions between an individual and their co-workers. Meanwhile Barling et al. (2002), defined socialization as “conversations, observing behaviour of co-workers and the consequences of certain behaviour”. The workers daily interactions in the workplace have an impact on individual work behaviour. The training programme learned by an individual will shape the expectations about the job (Mullen, 2004). According to Chan et al. (2005), organizational policies and procedures are actually enacted with reference to their peers, so that socialization may affect the ISCB. Therefore, we hypothesize the third hypothesis as follows:-

H3: *CWS has a positive effect on ISCB.*

Individual Factors

Computer Self Efficacy (CSE)

Self-efficacy in IS can be defined as “a belief in one’s capability to protect information and information systems from unauthorized disclosure, modification, loss, destruction, and lack of availability” (Rhee et al., 2009). Meanwhile according to Bandura (1977), self-efficacy refers to the belief in the ability to perform a specific task by an individual. In order to perform a task, Chan et al. (2005) believed it can be developed through the past experience that one has received. Sasse, Brostoff and Weirich (2001) discussed the issues in security design, which includes characteristics of the technology and users, users' goals and tasks, the working context and how human/computer interaction can be used to address these issues. According to them, users must have knowledge (self-efficacy) of security issues and must be motivated to use security measures. In addition, security mechanisms must be matched to users’ capabilities and tasks. They also suggested creating the motivation for security through the physical, social and organizational environment. In order to increase users' knowledge and motivate them, Sasse et al.(2001) proposed the use of training, punishment and reporting security related incidents. Thus, the fourth hypothesis of this study is as follows:

H4:*CSE has a positive effect on ISCB.*

IS Perception (ISP)

Campbell and Beaty (1971), defined ISP as “the employee’s perception of the current organizational state in terms of IS as evidenced through dealings with internal and external stakeholders”. McLean (1992) argued that changing employees’ values, perceptions and behaviour is necessary in order to achieve a satisfactory level of IS security. The study explored factors affecting human behaviour and attitudes and how a change in them can be enforced through the aid of a security awareness campaign. Such considerations, to some extent, shows that IS security has a socio-technical role. Vyskoc and Fibikova (2001) presented a socio-technical view of information system security. The aim being to identify users’ perceived information system security. In addition, they considered information system security as a people related problem. The study thereby underlines the importance of the human aspects of information system security. Thus, the fifth hypothesis of this study is as follows:

H5:*ISP has a positive effect on ISCB.*

Personal Innovativeness (PI)

Rogers (2003) defined an innovation as “an idea, practice, or object that is perceived as new by an individual or other unit of adoption”. He also defined innovativeness as “the degree to which an individual is relatively earlier in adopting an innovation than other members of his (social) system” (Rogers et al., 1971). Other researchers, like Agarwal et al. (1998), defined personal innovativeness as “the willingness of an individual to try out any new information technology”. Jia(2009) conducted research on personal innovativeness related to problematic technology use. He demonstrated that computer playfulness and personal innovativeness are two specific traits. These traits contribute to positive behavioural and affective outcomes. In this study, he suggests that personal innovativeness is a manifestation of openness to experience in the context of technology use.Rosen (2006) studied the effect of personal innovativeness in the domain of IT. He focused on the acceptance and use of technology to relate the personal innovativeness as a main-effect variable for the behavioural intentions. Thus, the sixth hypothesis of this study is as follows:

H6:*PI has a positive effect on ISCB.*

Research Methodology

The purpose of this study is to measure and evaluate the environmental, individual and behaviour's cognitive factors that influence the level of ISCB in the Malaysian Army based on SCT. We have developed the theoretical model for this research and added two factors in our study. Chan et al. (2005) considered that organization climate (UMP, DSP and CWS) is an independent variable for ISCB. The study also indicates that ISP and individuals with CSE can be considered as independent variables for ISCB. ISCB is the dependent variable for this research model. According to Griffin and Neil (2000), compliant IS behaviour refers to the set of core IS activities that need to be carried out by individuals to maintain IS as defined by IS policies. Therefore, Chan et al. (2005) suggested that to be able to carry out recommended (compliance) behaviour, an employee needs to be influenced by a conducive IS climate and the skills in order to perform the required actions. Figure 1 is the research framework for this study.

Selections of Measures

Measurement of the variables in the theoretical framework is an integral part of research and an important aspect of research design. All the variables are measured using a set of questionnaires developed by instruments that have been used in previous research. This is an inexpensive way to gather data from a potentially large number of respondents and the only feasible way to reach a large number of reviewers in order to allow statistically analysis of the results. A well-designed questionnaire that is used effectively can gather information on both the overall performance of the test system as well as the information on specific components of the system. The formulated questionnaire is used to collect data from the respondents who are normally the end users of IT in the Malaysian Army. The questionnaire consists of two sections. Section A collects the personal data and demographic profiles of respondents, such as rank, service duration, work experience, age, present appointment, skill qualification and academic qualification while Section B consists of questions pertaining to ISCB. Section B is divided into seven parts, namely, UMP, DSP, CWS, ISP, CSE, PI, and ISCB. A five-point Likert scale was used to measure these constructs. Scale 1 indicates 'Strongly Disagree', scale 2 denotes 'Disagree', scale 3 represents 'Neither Agree nor Disagree', scale 4 shows 'Agree', and scale 5 indicates 'Strongly Agree'. For this study, all constructs were adopted from previous research, such as Decker (2008), Martins and Eloff (2001), Hayes et al. (1998), Schnake (1983) Neal & Griffin (1997), Rhee, Kim and Ryu, (2009), and Chan et al. (2005). Table 1 summarizes the items used for all the constructs in the study.

Sampling Design

The aim of this research is determine the effect of organizational climate and individual factors towards ISCB. The sample population of this survey involves eight of the main corps in the Malaysian Army – Royal Malay Regiment (RMR), Royal Armour Corps (RAC), Royal Signal Regiment (RSR), Royal Engineer Regiment (RER), Royal Artillery Regiment (RAR), Royal Military Police Corps (RMPC), Royal Services Corps (RSC) and Royal Electrical and Mechanical Engineering (REME). In this research, the Cluster Sampling design technique is used to identify the sample because the target population for this research involves many units in the Malaysian Army, which are stationed in various locations. Sekaran (2006) suggested that the sample size of descriptive research is governed by the degree of precision and confidence required. However, in the study, the theoretical framework has a number of variables of interest, and the question is to determine what size sample would account for all factors. Krejcie and Morgan (1970) came up with a scientific guideline for sample size decisions to ensure a good decision model. According to them, based on the decision model table, this study needs a sample size of at least 400 out of the 80,000 personnel in the Malaysian Army. This is an appropriate sample size in order to establish the representatives of sample for generalizability of this study.

Data Collection Procedure

Since the questionnaire has never been tested in the Malaysian Army environment, a pre-test or pilot test had to be conducted before the questionnaires were distributed to actual respondents. The pilot test was conducted at Sungai Besi Camp, Kuala Lumpur on 1st Aug 2011. The author managed to obtain 30 samples from the participants of Institut Kejuruteraan Elektronik Tentera Darat. The results obtained were tested to confirm the validity and reliability of the questionnaires; also to get the feedback from the respondents regarding clarity of the questionnaire.

The pilot test involved a limited number of participants, as it was the researcher's intention to improve the instrument (if any) before it was tested against the bigger sample. Primary data were collected through questionnaires and interviews with the respondents. The survey was conducted over a one-week period from 12 Aug to 16 Aug 2011 by using the self-administered drop-off method and through the assistance of the Administrative Officers (AO) from various Corps in the Malaysian Army. The respondents who underwent the survey came from different units and corps. A total of 400 questionnaire forms were distributed, collected from the respondents and used in the analysis.

Data Analysis Technique

The data collected from the surveys were coded and entered into the Statistical Package for the Social Sciences (SPSS), version 18 for statistical calculation and analyses. The data collected were checked for completeness and proper data entry prior to other analyses. The Cronbach's Alpha was used to measure the reliability of the instruments. The multiple regression analysis was also used to report the results of regression of the independent variables against information security compliant behaviour. The suitability of the data for multiple regression analysis was assessed by investigating the relationship among the independent variables and dependent variable. In this study a statistical significance of p <=.05 is considered acceptable as it follows the generally accepted conventional social science research (Sekaran, 2003).

Findings

Demographic Profile

The demographic profiles of the respondents are gender, workplace, rank, age, corps, education background, working experience and length of service in current appointment, as shown in Table 2.

Reliability Test

The Cronbach's Alpha was used to measure the reliability of the instruments. According to Sekaran (2003), the closer the reliability coefficient gets to 1.0, the better the reliability. In general, a reliability coefficient of less than 0.60 is considered as poor, those in the range of 0.70 are acceptable and those above 0.80 are considered as good. Table 3shows that the results of Cronbach's alpha were between 0.626 and 0.855.

Correlation Test

In this study, a correlation test was conducted to examine the relationships between the dependent variable, ISCB and the individual independent variables namely UMP, DSP, CWS, CSE, ISP and PI. The Pearson correlation is used to explore the relationship between two variables. This will give an indication of the relationship direction whether it is positive or negative and also the strength of the relationship (Pallant, 2011). From Table 4, it was found that all the independent variables are significantly positively correlated with ISCB. The strongest correlation was between ISCB and ISP with r=0.629 and the weakest was between ISCB and DSP with r=0.476.

Multiple Regressions

In this study an analysis of the effect of all independent variables (UMP, DSP, CWS, CSE, ISP and PI) on the dependent variable (ISCB) was conducted. The intention was to identify which independent variable is stronger in determining ISCB in the Malaysian Army environment. This analysis can establish that a set of independent variable explains a proportion of variance in the dependent variable at a significant level (R square) and the relative predictive importance of the independent variable by comparing beta weights (Garson, 2005).

The purpose of multiple regression test is to identify which independent variables are stronger in determining ISCB. The ANOVA result on Table 5 shows that the model in this study reaches statistical significance. It indicates that the model as a whole is significant [F (6,393) = 78.7, p = 0.000]. Table 6 shows that the correlation of the independent variables with dependent variable is strong with R = 0.739. The R Square value shows that 54.6 percent of the variance in ISCB could be explained by all independent variables in the study namely UMP, DSP, CWS, CSE, ISP and PI.

An examination of t-values in Table 7 shows that only four independent variables (CWS, ISP, CSE and PI) are making a statistically significant contribution to the prediction of the dependent variable (ISCB). The beta coefficient in multiple regression tests indicates how strongly the independent variables could predict the dependent variable.

The result shows the largest beta coefficient is 0.327, which is for ISP. It indicates that ISP is the strongest contribution to dependent variable (ISCB) if compared to CWS, CSE and PI in this model.

Meanwhile the beta values for CWS and CSE were the lowest (0.198) which indicate that they made the least contribution to ISCB.

Discussion and Conclusion

In this study, it was found that only CWS reach a statistically significant unique contribution to the prediction of the dependent variable (ISCB). Others independent variables in organization climate namely UMP and DSP were not significant. The majority of respondents believe that the management within their respective units are not very serious about information security and that the officers or senior ranks do not always discuss information security policies with them. From the direct supervisory aspect, we found that officers or senior ranks do not update their soldiers on changes to information security procedures through direct verbal communication or via communication tools. Meanwhile, they also believe that co-workers socialization would report breaches of information security to superiors and take information security seriously.The results found that users' perception on how the Army units management seriously influence their employees behaviour towards IS compliance. This is supported by Parker's (2003) statement that the measurement of management factors by the end user's only determines the perception of how the management emphasize security awareness in their environment. The study also found that all individual factors, namely, CSE, ISP and PI play an important part in order to perform their compliance behaviour.A summary of the results is shown in Table 8.

The majority of respondents believe that it is not safe to reveal their login information to anyone or for any reason. They also believe that protecting confidential information stored in their computer will reduce illegal access to it. Meanwhile, from the innovativeness aspect, they tend to look for ways to experiment with new information technology, especially on IS if they have heard about it. These results also determine the users' perception on themselves towards IS. This is about what they believe, such as perception or a higher willingness to study new technology, knowledgeable about information technology and understanding their role in protecting information, the ability to identify a breach in IS and comply with information security procedures and behaviour.This result provides some information and guidelines to the army top management on which areas they should emphasize and take actions according to priority to increase the ISCB among the soldiers. In this case the users' perception on IS should be emphasized by the management to achieve higher ISCB in the Army.

Implications

As for theoretical contribution, the study provides evidence on how the social cognitive theory is combined with organizational and individual factors to study compliance in a secured organization. Detailed planning and a programme should be implemented by top management in the Malaysian Army. Despite the different roles and responsibilities that come with different levels in the organisation, all these users use information systems or the information it produces. This means that at some level, these users are all end-users and need to be made aware of the security issues required at this level (O'Brien, 1999). In order to increase the level of security within the unit and corps, top management should frequently look at implementing policies and provide training programmes. The management needs to educate the army personnel as end-users in security awareness and implement management policies to every unit and IT department. Since the security policy of the organisation sets the security direction for the organisation, knowledge of this policy will help the personnel to understand what the organisation is striving for concerning information security. The ideas behind many information security policies are similar from organisation to organisation (Wood, 1994). The Army personnel as end-users should be taught basic information security concepts. This knowledge will stand them in good stead when trying to understand the threats to and vulnerabilities of computer systems. It will also aid understanding of the procedures learned. The material should include basic information security concepts, such as confidentiality, availability and integrity (USA Dept. of Commerce, 1998).

Research Limitation and Future Research

Since this survey is confined to eight corps, it may limit the generalizability of the findings to the Malaysian Army organization as a whole.

It is suggested that further research should be carried out to extend the finding of this study to all corps (16 corps) in the Malaysian Army. Future research should also look into other factors, such as training, policies, loyalty, technology or other variables that are related to this study.

References

Agarwal R. and Prasad J. 1998.A conceptual and operational definition of personal innovativeness in the domain of Information Technology.*Information Systems Research,V*ol. 9, no. 2:204-215.

Aytes K. and Connolly T. 2003.A research model for investigating human behaviorrelated to computer security, Proceedings of the Ninth Americas Conference on Information Systems: 2027-2031.

Bandura, A. 1997.*Self-efficacy: The exercise of control,* New York: Freeman.

Bandura, A. 1989. Social cognitive theory. In R. Vasta (Ed.), *Annals of child development.Vol.6. Six theories of child development* (pp. 1-60). Greenwich, CT: JAI Press.

Barling, J., Loughlin, C. and Kelloway, K. 2002.Development and test of a model linking safety specific transformational leadership and occupation safety.*Journal of Applied Psychology,Vol. 87, no. 3:* 488-496.

Beland, F. and Dedobbeleer, N. 1991.A safety climate measure for construction sites.*Journal of Safety Research, Vol. 22, no. 2:*97-103.

Campbell, J.P., Dunnette, M.D., Lawler, E.E. III. &Weick, K, Jr. 1970.*Managerial behavior, performance and effectiveness.*New York, McGraw-Hill.

Campbell, J.P. and Beaty, E.E. 1971.Organizational Climate: Its measurement and relationship to work group performance. Paper presented at the Annual meeting of the American Psychological Association, Washington D.C.

Colwill, C. 2010. Human factors in information security: The insider threat-who can you trust these days?" *Information Security Technical Report.*

Chan, M., Woon, M.Y. and Kankanhalli, A.2005. Perceptions of information security in the workplace: Linking information security climate to compliant behaviour. *Journal of Information Privacy and Security,* Vol. 1, no. 3: 18-41.

Compeau, D. and Higgins, C.A. 1995. Computer self-efficacy: Development of a measure and initial tests," *MIS Quarterly,*Vol. 19, no. 2*:*189-211.

Garson, B. 2005. Work addiction in the age of information technology: An analysis. *IIMB Management Review,* Vol. 15: 21.

Glanz, K., Rimer, B.K. and Lewis, F.M. 2002.*Healthbehavior and health education. Theory, research and practice.* San Fransisco: Wiley & Sons.

Griffin, M.A. and Neal, A. 2000. Perceptions of safety at work: A framework for linking safety climate to safety performance, knowledge and motivation. *Journal of Occupational Health Psychology,*Vol. 5, no. 3:347-358.

Hayes, B.E., Perander, J., Smecko, T. and Trask, J. 1998. Measuring perceptions of workplace safety: Development and validation of work safety scale. *Journal of Safety Research,* Vol. 29, no. 3:145-161.

Brady, J.W. 2011.Securing health care: Assessing factors that affect HIPAA security compliance in academic medical centers.Proceedings of the 44th Hawai International Conference on System Sciences.

Jia, R. 2009.*Problematic technology use: A negative outcome of computer playfulness and personal innovativeness?*Proceedings > Proceedings of JAIS Theory Development Workshop.*Sprouts: Working Papers on Information Systems*, 9(45). http://sprouts.aisnet.org/9-.45.

Krejcie, R.V. and Morgan, D.W. 1970. Determining sample size for research activities.*Educational and Psychological Measurement*, Vol. 30: 607-610.

McCue, K. 2008. A comparison of employee benefits data from the MEPS-IC and form 5500. Working Papers 08-32, Center for Economic Studies, U.S. Census Bureau.

Decker, L. G. 2008.Factors affecting the security awareness of end-users: A survey analysis within institutions of higher learning. Unpublished thesis.Capella University.

Martins, A. andEloff, J.H.P. 2001.Measuring information security.Proceedings of Workshop on Information Security - System Rating and Ranking, Virginia.

Mathisen, J. 2004. Measuring information security awareness – A survey showing the Norwegian way to do it.Unpublished Master thesis, NISlab Norwegian.

McLean K. 1992. IS security awareness - selling the cause. Proceedings of the IFIP TC11, 8th International Conference on IS security, IFIP/Sec '92.*Conference (part 1), Vieweg*: 49–58.

Mullen, J. 2004.Investigating factors that influence individual safety behavior at work.*Journal of Safety Research,* Vol. 35, no. 3:275-285.

Murray, B. 1991. Running corporate and national security awareness programmes. Proceedings of the IFIP TC11 Seventh International Conference on IS security: 203-207.

Neal, A. and Griffin, M.A. 1997.Perceptions of safety at work: Developing a model to link organizational safety climate and individual behavior. Paper presented at the 12th Annual Conference of the Society for Industrial and Organizational Psychology, St. Louis, MO.

O'Brien, J.A. 1999. *Managing information systems: Managing information technology in the internetworked enterprise (4th ed.)*. United States of America: Irwin/McGraw-Hill.

Pahnila, Siponen and Mahmood. 2007. Employees' behaviortowards IS security policy compliance.Proceedings of the 40th Hawaii International Conference on System Sciences.

Pallant, J. (2011). *SPSS SURVIVAL MANUAL - A step by step guide to data analysis using SPSS*. Australia: Allen & Unwin

Parker, D.B. 2003.Motivating the workforce to support security.*Risk Management Magazine, Vol. 50, no.* 7: 16-19.

Rhee, H.-S., Kim, C., and Ryu, Y. U. 2009.Self-efficacy in information security: Its influence on end users' information security practice behaviour.*Computers & Security: 1-11.*

Rogers, E.M. 2003. D*iffusion of innovations (5th ed.)* Free Press: New York.

Rogers, E.M and Shoemaker, E. 1971.*Communication of innovations, a cross-cultural approach*.The Free Press, 2nd edition, New York.

Rosen, P.A. 2006. The effect of personal innovativeness on technology acceptance and use.Unpublished Academic Dissertation, Graduate College of the Oklahoma State University, USA.

Sasse A, Brostoff, S. and Weirich, D. 2001.Transforming the 'weakest link' a human / computer interaction approach to usable and effective security.*BT TechnologyJournal*, Vol. 19, no. 3: 122-131.

Schnake, M.E. 1983. An empirical assessment of the effects of affective response in the measurement of organizational climate.*Personnel Psychology,*Vol. 36, no. 4:791-807.

Sekaran, U. 2006. *Research methods for business: A skill building approach.* New York: John Wiley & Sons, Inc.

Sekaran, U. 2003. *Research methods for business* (4th ed.). Hoboken, NJ: John Wiley & Sons.

Straub, D.W. 1990. Effective IS security: An empirical study. Information Systems Research, Vol. 1, no. 3: 255-276.

United States of America. Dept. of Commerce. 1998. Information security training requirements: A role- and performance-based model. Washington: U.S Government Printing Office.

Vyskoc, J. and Fibikova, L. 2001. IT users' perception of IS security.Proceedings of the IFIP WG 9.6/11.7 Working-Conference.

Wood, C.C. 1994. Information security policies made easy. Ohio: Bookmasters

Zohar, D. and Luria, G. 2003. The use of supervisory practices as leverage to improve safety behavior: A cross-level intervention model. *Journal of Safety Research, Vol. 34, no. 5:*567-577.

Figure 1: ISCB Research Framework

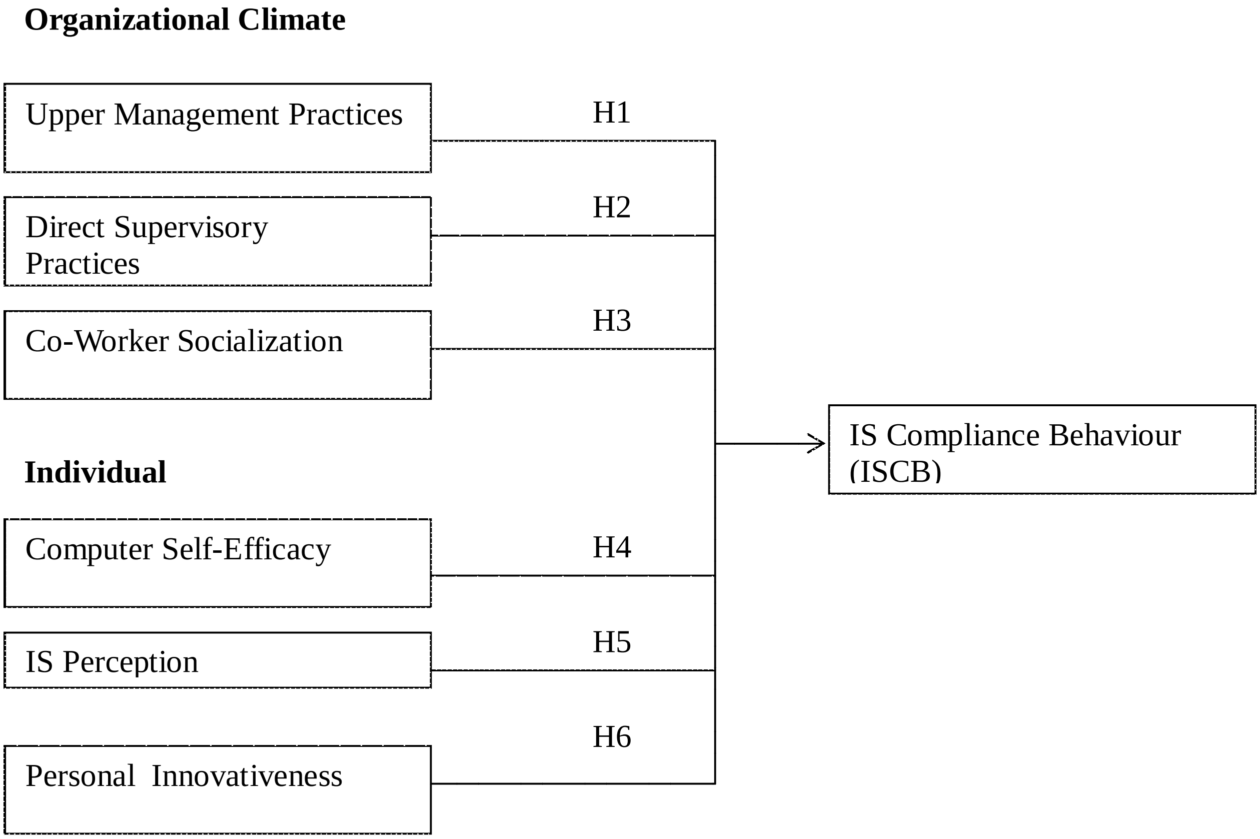

Table 1: Selection of Measures

Upper Management Practices		*Source*
Mgmt1	Management within my organization is very serious about information security.	Decker (2008)
Mgmt2	Information security training is included as part of orientation for new employees.	Decker (2008)
Mgmt3	Information security policies are discussed during my annual evaluation.	Decker (2008)
Mgmt4	Employees in my organization receive updated information or training regarding information security.	Decker (2008)
Mgmt5	My organization educates me on the importance of information security.	Martins and Eloff (2001)
Direct Supervisory Practices		
Sup1	My supervisor updates me on changes to information security procedures,e.g., through direct verbal communication or via communication tools.	Hayes et al. (1998)
Sup2	My supervisor discusses information security issues with me and my co-workers.	Hayes et al. (1998)
Sup3	My supervisor praises me when I adopt proper information security practices.	Beland and Dedobbeleer (1991)
Sup4	My supervisor considers information security compliance as a key factor in assessing my overall performance.	Chan et al. (2005)
Co-Worker Socialization		
Cowork1	My co-workers take information security seriously.	Decker (2008)
Cowork2	Co-workers tend to ignore information security procedures when rushing deadlines (reverse).	Hayes et al. (1998)
Cowork3	Co-workers discuss information security issues with me.	Hayes et al. (1998)
Cowork4	Co-workers would report breaches of information security to superiors.	Hayes et al. (1998)
Perception of Information Security		
Perp1	The organization sets high standards for the protection of its information assets.	Schnake (1983)
Perp2	Management is concerned with information security of the organization.	Neal and Griffin (1997)
Perp3	My supervisor is concerned with information security of the organization.	Neal and Griffin (1997)
Perp4	My co-workers are concerned with information security of the organization.	Neal and Griffin (1997)
Self Efficacy		
Effi1	I believe that protecting confidential information stored in my computer will reduce illegal access to it	Rhee, Kim and Ryu (2009)
Effi2	I believe that it is not safe to reveal my login information to anyone, for any reason.	Rhee, Kim and Ryu (2009)
Effi3	I am able to identify a breach in information security even if there is no one to help me.	Compeau and Higgins (1995)
Effi4	I am able to identify a breach in information security, even if I do not have a copy of written procedures and rules to refer to.	Compeau and Higgins (1995)
Effi5	I am able to identify a breach in information security even if I have not seen a similar situation occurring before.	Compeau and Higgins (1995)
Personal Innovativeness		
PI 1	If I hear about a new information technology (especially on Information Security), I would look for ways to experiment with it.	Agarwal and Prasad (1998)
PI 2	Among my peers, I am usually the first to try out new information technologies (such as antivirus).	
PI 3	I like to experiment with new information technologies especially on information security.	
PI 4	In general, I am hesitant to try out new information technologies.	
Information Security Compliance Behaviour		
Comply1	I will comply with information security procedures when performing my daily work.	Hayes et al. (1998)
Comply2	I tend to ignore information security procedures that I think are not necessary.	Hayes et al. (1998)
Comply3	I tend to ignore information security procedures in order to complete my work quickly.	Hayes et al. (1998)
Comply4	Sometimes I do not comply with information security procedures when it affects the performance/ productivity of my work	Chan et al. (2005)
Comply5	I tend to comply with information security procedures only when it is convenient to do so.	Chan et al. (2005)
Comply6	I tend to ignore information security procedures when I am busy	Chan et al. (2005)

Table 2: Summary of Respondents' Demographic Profile

Items	Group	Frequency	Percent
Gender	Male	281	70.3%
	Female	119	29.8%
	Total	400	100%
Age Group	Less 20 yrs	12	3%
	21 – 30 yrs	238	59.5%
	31 – 40 yrs	124	31%
	More 40 yrs	26	6.5%
	Total	400	100%
Length of Service	Less 5 yrs	100	25%
	6 – 10 yrs	114	28.5%
	11 – 15 yrs	84	21%
	More 15 yrs	102	25.5%
	Total	400	100%
Academic Level	Degree and above	36	9%
	Diploma	34	8.5%
	SPM	280	70%
	PMR	50	12.5%
	Total	400	100%
Attended IT Course	Yes	145	36.3%
	No	255	63.8%
	Total	400	100%
Attended IS Course	Yes	24	6%
	No	376	94%
	Total	400	100%
Rank	Officer	54	13.5%
	Senior Rank	96	24%
	Lower Rank	157	39.3%
	Private	93	23.3%
	Total	400	100%

Table 3: Reliability Coefficients

Variables	Cronbach's Alpha
UMP	0.809
DSP	0.812
CWS	0.746
ISP	0.855
CSE	0.778
ISCB	0836
PI	0.806

Table 4: Correlations Table

		UMP	DSP	CWS	CSE	ISP	PI
ISCB	*r*	0.546**	0.476**	0.618**	0.564**	0.629**	0.548**
	Sig. (2-tailed)	0.000	0.000	0.000	0.000	0.000	0.000
UMP	*r*	1.000	0.673**	0.663**	0.429**	0.677**	0.476**
	Sig. (2-tailed)		0.000	0.000	0.000	0.000	0.000
DSP	*r*		1.000	0.612**	0.450**	0.529**	0.474**
	Sig. (2-tailed)			0.000	0.000	0.000	0.000
CWS	*r*			1.000	0.538**	0.646**	0.528**
	Sig. (2-tailed)				0.000	0.000	0.000
CSE	*r*				1.000	0.449**	0.613**
	Sig. (2-tailed)					0.000	0.000
ISP	*r*					1.000	0.412**
	Sig. (2-tailed)						0.000
PI	*r*						1.000
	Sig. (2-tailed)						

r= Pearson Correlation

**. Correlation is significant at the 0.01 level (2-tailed).

Table 5: Multiple Regression ANOVA

ANOVA[b]

Model	Sum of Squares	Df	Mean Square	F	Sig.
Regression	3032.095	6	505.349	78.666	.000[a]
Residual	2524.615	393	6.424		
Total	5556.710	399			

a. Predictors: (Constant), PI, ISP, DSP, CSE, CWS, UMP

b. Dependent Variable: ISCB

Table 6: Multiple Regression Results (Model Summary)

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.739[a]	.546	.539	2.535

a. Predictors: (Constant), PI, ISP, DSP, CSE, CWS, UMP

b. Dependent Variable: ISCB

Table 7 : Multiple Regression Coefficients

Coefficients[a]

Model	Unstandardized Coefficients		Standardized Coefficients		
	B	Std. Error	Beta	t	Sig.
1 (Constant)	4.174	.824		5.065	.000
UMP	.066	.062	.058	1.059	.290
DSP	-.069	.064	-.054	-1.081	.280
CWS	.283	.075	.198	3.760	.000
ISP	.429	.066	.327	6.494	.000
CSE	.218	.050	.198	4.320	.000
PI	.241	.061	.182	3.955	.000

a. Dependent Variable: ISCB

Table 8: The Summary of Research Objectives, Hypotheses and Findings

Research Objectives	Hypothesis	Findings
To determine the relationships and effects of organizational climate and individual factors towards ISCB in the Malaysian Army	H1: UMP has a positive effect on ISCB	Not supported
	H2: DSP has a positive effect on ISCB	Not supported
	H3: CWS has a positive effect on ISCB	Supported
	H4: CSE has a positive effect on ISCB	Supported
	H5: ISP has a positive effect on ISCB.	Supported
	H6: PI has a positive effect on ISCB	Supported

In information security observing end-user security behaviors is challenging. Moreover, recent studies have shown that the end users have divergent security views. The inability to monitor employee IT security behaviors and divergent views regarding security policies, in our view, provide a setting where the principal agent paradigm applies.Â @article{Herath2009EncouragingIS, title={Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness}, author={Tejaswini Herath and H. Rao}, journal={Decis. Support Syst.}, year={2009}, volume={47}, pages={154-165} }. Tejaswini Herath, H. Rao. Individual behavior is influenced by a wide variety of organizational system and resources. Systems such as the organizational structure and hierarchy strongly influence and constrain both what individuals do and how they do.Â Organizational culture and climate also affect an individualâ€™s behavior at work. The various dimensions of organizational culture are values, ethics, beliefs, climate and culture.Â Individuals who experience frequent layoffs are more likely to be motivated by factors that affect job security, while other individuals would consider job security to be relatively unimportant and would be motivated by other factors.Â In addition to changing employment opportunities, technological change has its effect on job design. security climate, security compliance, information security, social network analysis, social influence. 1 Introduction.Â The formation of organisational climates can be analysed by adopting the theoretical lens of the interactionist perspective (Schneider and Reichers 1983). This perspective draws on symbolic interactionism to explain how organisational climates could be socially constructed as the employees interact with their workgroup (Ashforth 1985). This explanation fits our conceptualisation of ISC.Â Normative social influence offers prescribed behaviours and beliefs that regulate climate by removing disagreements. These social influences provide a theoretical ground for identifying the relevant interactions that affect security beliefs and behaviours. A. Personal factors â€“ The personal factors that can influence the behavior of an individual is further categorized into 2 parts that includes Biographic and learned characteristics. 1. Biographic Characteristics â€“ Every human being have certain type of characteristics which are inherited and genetic in nature. These characteristics cannot get changed.Â Also, it is considered as the process which allows the information to enter in the minds and allowed to obtain sensible meaning for the whole world. (3)Values â€“ Values are considered as the global belief that instructs different judgments and actions across various situations. It consists of an individualâ€™s idea based on the right, good and desirable opinions.