FACTORS INFLUENCING STUDENTS' PERCEPTION ON INFORMATION SECURITY PLAN IN UUM

BABATUNDE DORCAS ADEBOLA

UNIVERSITI UTARA MALAYSIA

2010

FACTORS INFLUENCING STUDENTS' PERCEPTION ON INFORMATION SECURITY PLAN IN UUM

A thesis submitted to the college of business postgraduate studies

In fulfillment for the requirement of a degree in

Msc International Accounting

By

BABATUNDE DORCAS ADEBOLA

(802478)

COLLEGE OF BUSINESS

UNIVERSITI UTARA MALAYSIA

2010

PERMISSION TO USE

In presenting this thesis in partial fulfillment of the requirements for a Post Graduate degree from the Universiti Utara Malaysia, I agree that the Library of this University may make it freely available for inspection. I further agree that permission for copying of this thesis in any manner, in whole or in part., for scholarly purposes may be granted by the Lecturer or the Lecturers who supervised my thesis work or, in their absence, by the Dean of the Graduate School which my thesis was done. It is understood that any copying or publication or use of this thesis or part thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to the Universiti Utara Malaysia in any scholarly use which may be made of any material in my thesis.

Request for permission to copy or to make other use of material in this thesis in wholly or in part should be addressed to:

Dean of Postgraduate

College of Business

Universiti Utara Malaysia

060 10 Sintok

Kedah Darul Aman

ABSTRACT

This thesis seeks to determine the factors influencing information security plan in Universiti Utara Malaysia (UUM). Although, there are various means by which higher institutions of learning in Malaysia have implemented technical solutions to protect information from various ways in order to prevent internal security breaches. Therefore, an approach which would be emphasized and determine information security plan within higher institutions is much needed to make an impact on the day to day security task of the employees.

ACKNOWLEDGEMENT

This project would not have been complete without the guidance, support and encouragement of numbers of individuals. First and for most, my gratitude goes to Associate Professor Dr. Tayib Mohammad, and Associate Professor Dr. Noor Azizi Ismail, for making me feel at home in Malaysia, and for their support and encouragement in making my studies in UUM valuable and attainable.

Also, my appreciation goes to my supervisor, Dr Mohamad Hisyam Selamat for his continued guidance, interest, support, as well as patience and time to go through my write up and the valuable suggestions he provided to make this thesis a success. I cannot but appreciate Dr Shamir Abdullah Sivaraj for his efforts to review the project and his invaluable support and encouragement.

My appreciation goes to the COB assistant registrar Mr. Roslee Mardan and Madam Asamah Din, CAS assistant registrar Ms Yati Arikah, and Mr. Idris from COLGIS who make the colleges' information available for me to use. And Universiti Utara Malaysia who allowed me to do my case study at their institution, also the students who out of their willingness helped me to filled my questionnaires without much ado. Without their permission, I would not have

completed my studies. To all my loving and caring friends in UUM for sharing moments, the wonderful knowledge and experience impacted will not only be useful now but in the nearest future.

My hearty thanks goes to my darling husband Daniel Babatunde for the love, encouragement and financial support during the course of my study .I cannot but show my appreciation to my Children Dannie, Daniella and Jessie for their kindness, support, love, encouragement, understanding in making my studies a success.

TABLE OF CONTENTS

CONTENTS **PAGE**

CHAPTER ONE

INTRODUCTION

1.1 Research Background

One of the primary goals of information system is to make sure that the investments in information security system generate business value. It also mitigates the risks that are associated with information system. This can be done by implementing an organizational structure with well-defined roles for the responsibility of information, business processes, applications, infrastructure and others. Decision rights are a key concern of IT governance. Weill and Ross (2004) suggested, depending on the size, business scope and IT maturity of an organization, centralized, decentralized or federated models of responsibility for dealing with strategic IT matters. On this note, a well defined control of information security plan is the key to success in any establishment.

The security plan will not only address the issues of vulnerability, which represent a high level of risk , also the implementation of a security policy which define how security issue should be handled. The security policy should address the appropriate use of the organizational resources,

the requirements on individuals who request and maintain accounts, the acceptable methods of remotely connecting to the organizational LAN, the ways information is protected from unauthorized access, disclosure, corruption, and loss, the procedures for adding new devices to the network, and the rules regarding the use of privileged system accounts (Oppenheimer et al., 1997).

The security policy should be periodically reviewed in order to ensure that an appropriate assurance level is maintained. Also the security policy should include appropriate procedures for handling and responding to security incidents and natural disasters, and appropriate hiring practices for minimizing employee-related threats. Thus the definition of , information security plan that has been evolving rapidly over the last few years and it comprises of security awareness, policy formation and development.

An information security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned responsibilities and expected behavior of all individuals who access the system. The information security plan should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system. It should reflect input from various managers with responsibilities concerning the system, including information owners, the system operator, and the system security manager. Additional information may be included in the basic plan and the structure and format organized according to agency needs, as long as the major sections described in the document are adequately covered and readily identifiable.

The information security plan is a statement that protects an identified resource from an unauthorized use. The security of an information system involves the availability, confidentiality and integrity of its data and its functionality (INFOSEC, 1993). Therefore institutional security plans should be put in place to safeguard information from threat, such as malicious authorized users, negligent authorized users as well as outsiders. (Meyer et al.,(1995).

The previous studies show that Malaysia Universities are yet to fully implement strategic information security plans (Ismail et al 2007). David Burrill, Head of Group Security British American Tobacco says that "what we're doing is lurching from challenge to challenge, from crisis to crisis" (as quoted in Scalet, 2005). Stan Gatewood, CISO of the University of Georgia (as quoted in Scalet, 2005), says that "If you have no security plan, how will you know if you're doing it right? You will be reacting to every little thing that bumps in the night," All these statements highlight that Malaysian Universities need to establish information security plan.

Due to the importance of information security plan in any organizations, including higher education institution, researcher intends to obtain the perception of UUM students on UUM's information security plan. This is because they are the main stakeholders in the University.

1.2 Problem statement

Security is not a single solution but a pervasive ongoing process of reviewing and revising based on changes happening surrounding the organization, including UUM. Nor Haryani (2005)

stated that security is the culmination of interaction between people, process and technology. Andress (2002) argues that people are the most important security component. Educating and rewarding users on security awareness is a great way to build conscious environment. In the University, people such as employees, students, academician from security as they form an integral part of security system. This was further supported by Russell (2002) whereby he said that people are often overlook as part of security component. He identified three main requirement of security to be:

i. Confidentiality: The aspect of computing system is accessible only by the authorized parties.

ii. Integrity: The asset can be modified only by authorized or only in authorized way.

iii. Availability: The assets are accessible to authorized parties or only in authorized ways.

Educational institutions must realize the need to incorporate not only the students, but the staff and the decision maker as information system is everyone's responsibility not just the information technology section/ department. It is also imperative that the users should understand not only how to protect the information but why protecting staff, students' information is very important. According to Andress (2000), and Krutz (2001), the combination of people, process and technology to provide security to the organization equally considered important and thus each of them must be given the same attention. Rusell (2002) emphasize the need why people as employees/staffs in the organization must understand how their actions can greatly impact the overall security position of an organization.

With security breaches on the very rise and lots of computers hackers everywhere, an organization must put in place strong security measures to survive. Apparently, higher institution of learning do not take information security to be paramount knowing well that protecting information is more or less like protecting the entire organization (Baltzan /Philips et al., (2008). Enron Company could have still been in existence today if its information had not been destroyed. But with the promulgation of Sarbanes Oxley Act (SOX Act 2002), loss of organizational information system would be protected whatever misappropriation from the management level. Without Information security plan, argued by Von Solms (2000), the organizations are exposed to security threat and vulnerabilities and this inevitably lead to security incidents. Researchers in information system area regard human factor as the weakest link in security solution (Perry, 1985, Angel 1993).

To recapitulate, involving human in ISP is paramount importance. Before reaching this stage, knowing their perception on ISP is necessary. This research aims to assist in this process by studying the perception of UUM students on ISP.

1.3 Research Question

Based on the above discussion, this research intends to answer the following research question.

1).What are the factors that influence UUM students' perception on information security plan?

1.4 Research objectives

Based on the above research questions, the following research objectives are developed as a benchmark:

1. To identify perceptional factors that may affect an information security plan.

2. To develop a framework based on the identified perceptional factors of information security plan. To identify if the missing plan present needs should be verify.

3. To validate the framework from the perspective of UUM.

1.5 Significant of the study

This study may give a useful feedback to students, the staffs as well as the management of UUM. The useful feedback may assist the decision maker to plan for information security plan both on long and short terms. However, many organizations overlook the significant leverage to be gained from effective use of information security plan. Apparently, this study will not only alert the institution but safeguard its information. Therefore, the security of such information is very paramount in case of any unprecedented occurrence or threat and vulnerabilities.

1.6 Scope, limitation and assumption

The study is limited to one of the higher institution in Malaysia, namely, UUM. The degree of sampling and non sampling error may occur at minimum level of operations and functionalities in terms of departments within the organization. All respondents are assumed to know a bit if not all about information security plan.

1.7 Organization of the study

The remainder of the dissertation is divided into four chapters. Chapter 2 provides a review of related literature about information system security plan. Chapter 3 emphasizes on the research methodology, which begins with the hypothesis , model specification, variable measurement and data collection. Chapter 4 presents the empirical findings and results obtained from the analysis. The last chapter provides the discussion and implications of the study as well as suggestions and recommendations for future research.

1.8 Summary

Based on the above discussion ,ISP is an important factor which organization must take cognizant of .Organizational risk cannot be over emphasize especially in the case of UUM, hence the need to critically considered ISP in order to avert the risk thereof.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter discusses the literature review of this research. The literature is utilized to develop the conceptual framework of this research. To ease the reader, a diagram of the framework is offered at the end of the chapter.

2.2 Definition of information security plan

Information system security is being defined as the protection of information against unauthorized disclosure, transfer, modification or destruction, whether accidental or intentional (Krause & Tipton 2002). When examining the prerequisite for information security, it is essential to look at the qualities of information needed to be preserved in order to ensure affordable security The concept of information system governance emerged in the late 1990s when Brown (1997) and Sambamurthy and Zmud (1999) wrote about the "IT governance arrangement and framework". They said that IT governance arrangements represent "an

organization's IT-related authority patterns". IT governance's objective is to define structures, processes, and mechanisms to define decision making rights and responsibility about main IT issues, to control and monitor the effectiveness of such decisions, and to mitigate IT-related risks in order to achieve an organization's objectives.

The question which needs an urgent answer:" Is information system plan different from IT management and IT controls"? In the normal circumstances, information security plans started by creating the awareness, formulating policies to meet different levels of corporate security policy- top management view ,organizational security policy -users views and technical security policy- designers view (Abrams and Bailey 1995). Tanenbaum (1992) emphasize the separation between policy (what should be protected) and mechanism (how the policy is enforced). Therefore, it is hard to differentiate between information security plan and good management practices and IT control frameworks. ISO 38500 has helped clarify IT governance by describing it, as the management system used by directors. (2008 June - New ISO standard for Corporate Governance of Information Technology - World and The ISO 38500 IT Governance Standard .) In other words, IT governance is all about the stewardship of IT resources on behalf of the stakeholders who expect a return from their investment. The directors responsible for this stewardship will look to the management to implement the necessary systems and IT controls. Whilst managing risk and ensuring compliance are essential components of good governance, it is more important to be focused on delivering value and measuring performance.

Nicholas Carr et; al (2007) have emerged as a prominent critic of the idea that information technology confers strategic advantage. This line of criticism might imply that significant

attention to IT security plan is not a worthwhile pursuit for senior corporate leadership. However, Carr et al (2007) also indicates counterbalancing concern for effective IT risk management.

The manifestation of information security plan objectives through detailed process controls, e.g. in the context of project management, is a frequently controversial matter in large scale IT management. The difficulties in achieving a balance between financial transparency and cost-effective data capture in IT financial management e.g., to enable chargeback is a continual topic of discussion in the professional literature and can be seen as a practical limitation to information system security such as, IT steering committee/priority process, alignment with business objectives, IT strategy and architectural standards, IT project tracking support for strategic enterprise initiatives.

Financials can be measured in terms of operating budget, capital budget, asset management, resource allocation and planning. However, information security plan frameworks are such as information management policies corporate (privacy), business process owners, records retention, IT department, security, standards, practices and procedures, system documentation management, quality assurance ,regulatory compliance, escalation procedure, disclosure procedures and lastly contract administration and vendor management. Information security plan can take traditional IT management to a new level. Implicit in all these discussions regarding enterprise governance and information security plan is that, information security plan is not a new topic. Effective information security plan is a compilation of time-tested information

security management tools and techniques, although with a more enterprise wide perspective. The information system management and governance functions of the past have not changed dramatically but they and the enterprises they serve must perform to a much higher standard of due diligence.

Therefore, information security plan is an intellectual exercise that orchestrates all of the security concerns to make sure they are all being handled adequately on best practices common to all security. A well-balanced approach to information security plan consists of a variety of details, approaches and solution sets that match a particular organization's circumstances and requirements. There is a renewed focus on enterprise wide information and information-related technology issues that support enterprise security issues. Various industry tools can assist in orchestrating and executing technical elements of information system practices, but no tool is a total solution. For example, a key factor of information control is determining where it makes sense to centralize vs. decentralize components in a federated manner that fits the organization.

Enterprise security support, the IT components reflects the same core components as those found in overall enterprise security activities. IT management carries the responsibility of security within the IT department but must also play a larger role in executing the oversight of IT-dependent enterprise security activities. The message for senior management in any organization is that there is more to oversee in support of enterprise security than traditional IT management addresses, such as records retention or protection of intellectual assets where the information is not necessarily automated.

To recapitulate there is a need to establish an effective information security plan in the organization. As stated earlier, people are the most critical component information security plan. Thus every staff member must appreciate the effort to establish relevant and reliable security activities. To assist this process, understanding an individual's perception on information security plan is of paramount importance. Based on previous studies, there are four elements that influence an individual's perception in information security plan which are as follows:(1) size of the organization; (2) information system awareness and threat; (3) level of IT knowledge; and(4) business operation (Weill and Ross ,2004), Von Solms, (2000). The description of each element is provided in section 2.3 till 2.6.

2.3 Size of the organization

As organization's strategy changes over time, and has its unique security needs (Scweithzer,1992;Wood,1999). Therefore, such organization must meet its security needs by proposing three policies :

1. In high level reference which is the high level of overall plan embracing the general security goals and acceptable procedures..
2. In lower level reference, policies are defined information security methods of action that are selected from among alternatives and in the light of given conditions that that guide and determine present and future security decisions
3. The third level is Meta policy, with the aim of establishing how information securities policies are created, implemented and enforced. (Richard and Mikko, 2002).

As the implementation of information security plan involves cost, it is must be supported by adequate resources such as cash, experts and others. For example, Fenny et al (1992) found that information security activities must be monitored by chief information officer (CID) that report directly to chief Executive officer (CEO) to ensure its success. Implicit in this scenario is that large organizations are more capable of implementing information security plan. This is because large organizations have adequate cash, IT experts, capability and the need to establish effective and efficient information security plan compared with small and medium enterprises. Thus, there is a potential relationship between size of the organization and information security plan and in turn is included in this research theoretical framework.

2.4 Information security awareness and threat

Awareness as part of security plans is not only in training as it has been defined in 1989 in NIST SP 500-172 , but it creates the employees sensitivity to the threat and vulnerabilities of the system and the recognition of the need to protect data, information and the means of processing them. Therefore, awareness of the importance of information system will lead the management to plan organization information security. Stan Gatewood CISO of the University of Georgia (2005) says, if you have no security plan, how will you know if you're doing it right? You will be reacting to every little thing that bumps in the night. This is a research gap that this study intends to fill and also propose an information Security plan for higher institution especially in Universiti Utara Malaysia.

Information security is an integral part of corporate governance in raising the bar of corporate integrity and enhancing shareholder value. It goes beyond IT audit and beyond what the CIO can accomplish by himself/herself. (Fenny, et al., 1992), depending on the organization, information security plan may be the enabler for an organization to move to the next level or it may be the only way an organization can meet regulatory and legal requirements. In light of recent events and new Security Exchange Commission (SEC) regulations, corporate leaders will be more closely monitored and held accountable for their non actions. This new accountability includes significant fines and jail time. A continuing stream of regulatory actions on topics ranging from antiterrorism, anti -spam and privacy to document retention continually challenges enterprise of all sizes. In many cases, compliance must be obtained by use of technical solutions

Kwok and Dennis (1999) developed an information security model as part of a consultancy study for a banking organization, and this model has been extended in a collaborative research project with the National Australian Bank, funded by the Australian Research Council. The model was initially developed for risk analysis studies. And as illustrated in figure 1 It is therefore adapted in security audits in various organizations. In short, the model may serve as the essential security documentation for a security officer.

An essential feature of the model is that it represents, at any one time, the best set of security information available, and is therefore useful even when incomplete. When information is added to the risk data repository (RDR), it may be linked to existing components of the model, providing an essential level of cross reference, often omitted from paper documentation. It is postulated that the RDR could serve as an auditing conformance tool for the information security

management standards, in addition to its role in risk modeling. The model is hence described below in its current form, and then in relation to its potential role in information security management auditing.

In this role, the model not only represents the best set of information currently available to the security officer, it also highlights the entities that are relevant to the security officer, but which are not currently available in the organizational risk data repository . In figure 2.1, RDR essentially comprises three domains ; (1) environment- all those features that effectively host or support the operation of the information processing system (equipment, buildings, staff etc), (2) platforms- logical, description of information processing system and its defenses; and (3) assets- the data and processes are to be protected because misuse of these assets would have a deleterious effect on the business operations of the organization. From a risk viewpoint the model depicts the fact that an external threat will impact on the information processing systems' environment; thus, causing some potential effect on the operation of the system and if the defenses are inadequate then, causing some potential effect (disclosure, corruption, loss of availability) to the information assets which will, have some business impact. The model should contain sufficient information about its entities, and the links between the entities, to provide the best available information on the risks in relation.

To recapitulate, understanding information system awareness and threat could influence management when deciding to adopt or not to adopt information security plan. Thus, it is included in this research conceptual framework.

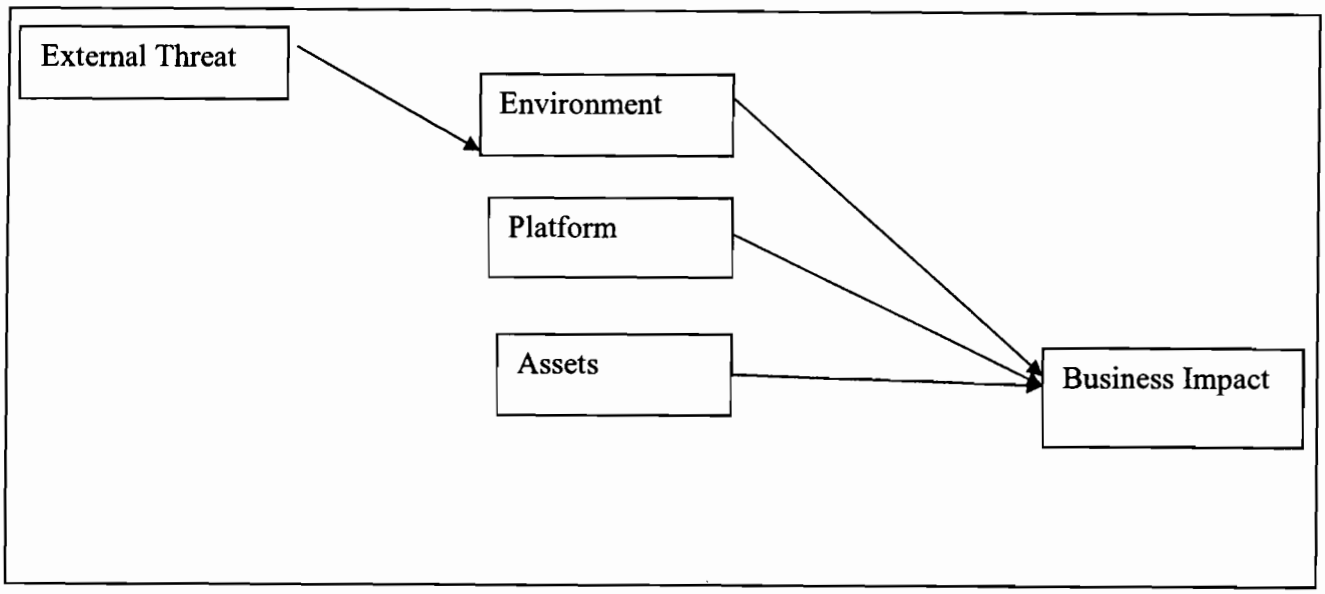

Figure 2.1: Risk data repository Model

2.5 Level of IT knowledge

Managing the IT function has become more difficult in recent years due to: increasingly sophisticated technologies, diversity of technology platforms and components in an organization, reduced time to market and time to respond to requirements of the business, new legislation and individual liability and reliance on IT as a critical enabler of many compliance, regulatory, corporate governance effectiveness and organizational effectiveness capabilities. Most of the managers agree on necessity of considering IT as an "organizational strategic player" (Boynton et al., 1994; Orlikowski and Barley, 2001; Sambamurthy, 2000; Venkatraman and Henderson, 1998).

These phenomena highlight that the effort to establish information security plan must be followed by an increase in IT knowledge. Being equipped with adequate IT knowledge enables the organization to implement information security activities effectively and efficiently. Thus there is a potential relationship between IT knowledge and information security plan. In turn, IT knowledge is included in this research theoretical framework.

2.6 Business operation

There is a strong relationship between business operation and ISP (Huston, 1992). This is because each industry inherits different levels of risk and threat. For example, financial sector requires higher ISP than educational sector. Nevertheless, due to the importance of giving accurate information to the students, it is expected that higher educational institution like UUM need an effective ISP as well. Thus the element is included in this research conceptual framework.

2.7 Conceptual Framework

Based on the above discussion, it is declared that the independent variables of this research consists of the following elements; (1) size of the organization; (2) information security awareness and threat; (3) level of IT knowledge; and (4) business operation. On the other hand,

the dependent variable is information security plan. The diagram of the relationship between independent variables and dependent variable is as illustrated in figure 2.2.

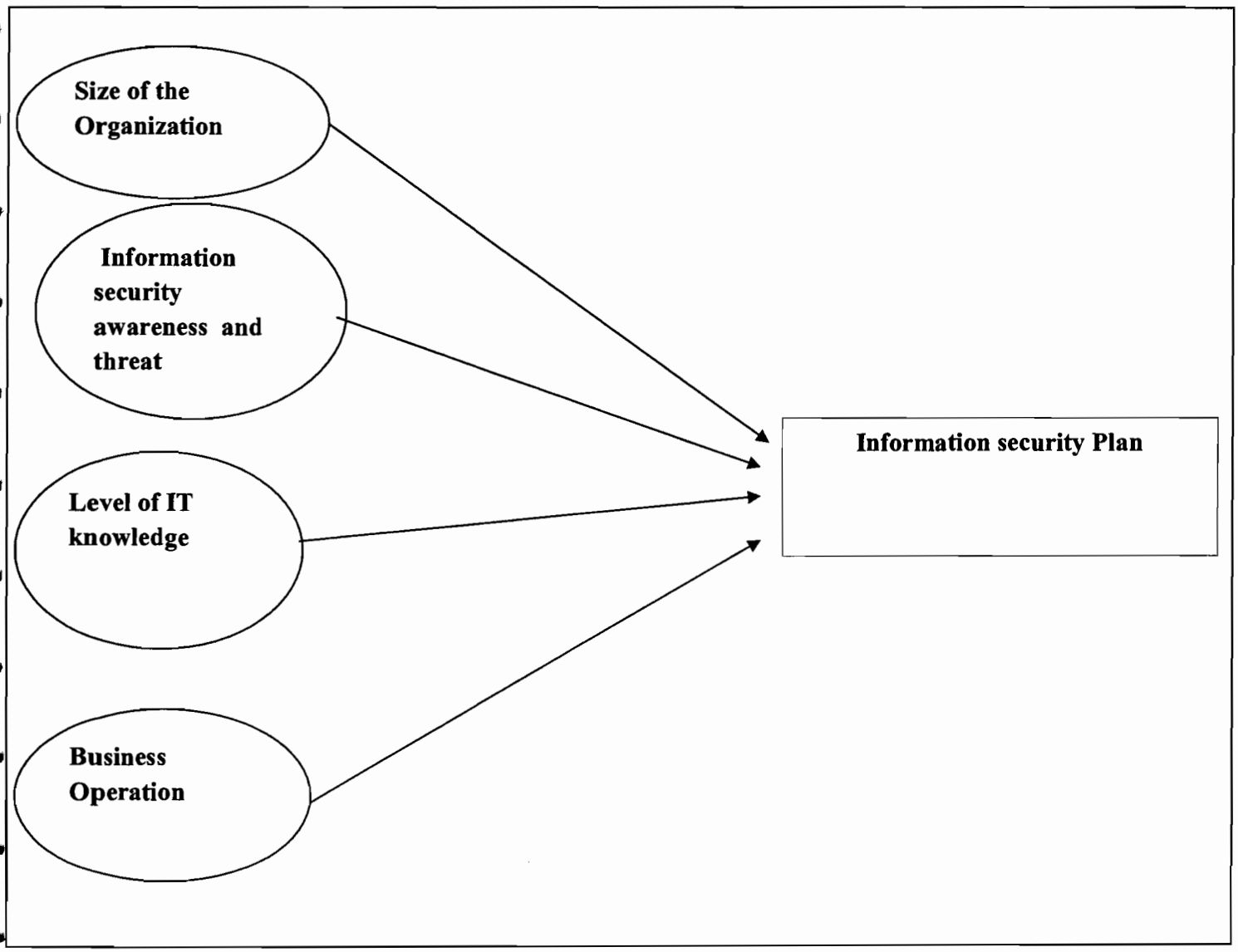

Fig 2.2 : Students Perception on factors influencing information Security Plan in UUM

2.8 Summary

In summary, this chapter discusses the literature that is related to information security plan. The focus of the discussion is towards the perception of individual on information security plan. The perceptional factors are relevant in this research are; size of the organization, information security awareness and threat level of IT knowledge; and business operation. To validate the framework, a systematic research methodology is dealt with in chapter 3.

CHAPTER THREE

RESEARCH DESIGN AND METHODOLOGY

3.1 Introduction

This chapter presents the methodology that was used to achieve the study objectives in chapter one and to test the study hypotheses. The discussions include research hypothesis, measurements of the variables, sampling and statistical techniques that were used to analyzing the data. A summary is offered at the end of the chapter.

3.2 Research Hypothesis

This section discusses the hypotheses that are developed in this research. The hypotheses are developed based on the framework that is illustrated in figure 2.

As stated in chapter 2, the first element of the framework is the size of the organization. There are many studies on size of the organization and information .The results are mixed. As the implementation of information security plan involves huge cost, it is expected that large organizations are more recline to adopt systematic information security plan. Thus, the following hypothesis is proposed.

H1: There is a positive relationship between size of the organization and information security plan.

The second element of the framework is information security awareness and threats. It is found that higher understanding on information security awareness and threat leads to the adoption of information security plan fenny et al; (1992). This is because the awareness on the potential risks or threats of information system in the organization motivates the management to have a sound information security plan. Thus the following hypothesis is proposed.

H2: There is a positive relationship between information security awareness and threat and security plan.

The third element is level of IT knowledge. Generally, agreed in the previous studies that an effective implementation of information security plan requires advanced IT knowledge Well and Ross,(2007). This is because nowadays information infrastructure is dominated by information and communication technologies. Thus there is a potential relationship between level of IT knowledge and information security plan. The proposed hypothesis is as follows:

H3: There is a positive relationship between level of IT knowledge and security plan.

The last element is business operation. There are many studies that investigate the relationship between business operation and information security plan such as Fenny et al;(1992), Wood,(1999) stated that there is positive relationship between business operation and

information security plan. However, Will and Ross(2007) found no relationship between business operation and information security plan. As each industry has different level of operational risks, its need for information security plan is different. Thus, the following hypothesis is proposed.

H4: There is a positive relationship between business operation and security plan.

Having determined the hypothesis for this research, the next section will discuss how each hypothesis is tested and validated.

3.3 Operational definition

The terms such as information security system, information security, information security management, computer security and information system are used interchangeably for this course of study. Therefore, the following terms are defined in the context of the thesis.

3.3.1 Information system security

The US National Security telecommunication and information system (NSTISS, 1992) defined information security system as that which is concerned with the protection of information against an unauthorized access to or modification whether in storage, processing or in transit. It is also concerned with the denial of services, including taking the necessary measures to detect document and as well counter threats to information system.

3.3.2 Information system

This is used in this study which is meant to be as a set of people, data and procedure that work together to provide useful information. The word 'system 'according to Senn, 1980:8 implies that the various components seek a common objective of supporting organization's activities. Therefore, an information system is involved with repertoires' of behavior in an organization.

3.3.3 Information system management

According to the international Federation of information processing (IFIP) working group (WG) 11.1,informationsecurity management covers a range of issues from both managerial and technical aspects that support the information security management Process (IFIP,1992). In other words, information security management addresses the operational, technical and human factors that affect information security (Kenning, (2001).

3.3.4 Information security

This term is often used interchangeably in this thesis with computer security and information security system. Nevertheless, there is a slight difference. Pipkin (2000) invariably argues that information security is much more than mere computer security. Information security is a multidimensional discipline that covers areas such as computer Science, Mathematics, philosophy, criminal justice, sociology accounting and Management (Wright,1998: Von

Solms,2001). Pipkin (2000) emphasizes that information security implies a business requirement to protect an organization's information assets.

Therefore, information security concerns protecting assets from disclosure, integrity violation and denial of service. However, Information security is widely used to describe security of information. For instance the term was used by US Department of Defense (D0D) in the Trusted Computer System Evaluation Criteria (TCSEC<1985) document, Office for Official publication of the European communities in the information Technology security Evaluation Criteria (TCSEC),1991) document, the British Standards Institute in the British Standards 7799 (BS7799,1999) documents, and the International Organization for Standardization in ISO17799(ISO,17799,2000) document.

Besides this, different authors, researcher and consultants (such as Peltier, 2001, Schultz et al, 2001: Pipkin 2000, Hone and Eloff, 2002 just to mention but few) prefer to use information security in place of security of information. According to Omar Bin Zakaria (2007) concluded by saying base on the above, information should be appropriate term to use when describing security of information.

3.3.5 Computer security

According to Gollmann (1999) states that ,it deals with the protection of computer systems and computer network system. Landwehr (2001) views it as a narrower topic than information security, which would cover all forms of information storage and processing. It means that computer security focus on computer based system or automated system security.

3.4 Research Design

This study aims to investigate the factors influencing security information plan in UUM. To undertake this type of quantitative research is considered relevant. Survey questionnaire was designed and distributed to get response from the selected sample. The questionnaire was distributed to three colleges, namely, UUM COB, UUM CAS and UUM COLGIS.

3.4.1 Research Equation

Based on the discussion in chapter 2, the following research equation is developed:

$$\triangle ISP \quad e = a + \beta SO + \beta ITK + \beta AT + \beta BO + e$$

Where

ISP = Information security plan

SO = Size of the organization

ITK = IT knowledge

ß BO = Business operation

a = Constant number of equation

ß = coefficient beta value

e = the residual error of the organization

3.4.2 Measurement

The questionnaires used in this study consist of 29 items, including both the demographic information and the factors considered. Size of the organization was constructed with 3 items, information security awareness and threat constructed with 5 items, level of IT knowledge constructed with 4 items, while business operation was measured with 3 items and the last construct which is information security plan was measured by 3 items.

A five-point likert scale ranging from (1) "not important" to (5) "very important" were employed to measure responses". The interval scale was used in this study because it is more suitable for measuring the magnitude of preference among individuals or students (Sekaran, 2003). Thus, reliability test was conducted on a selected sample of 100 students to verify the validity, correlation analysis, regression analysis. The questionnaire used in this study is attached in Appendix A.

3.4.3 Population and Sample

This study focuses only on the UUM students. Therefore the population constitute a total number of 20,157 and the research sampling was based on 100.The population frame will includes all the colleges (COB,CAS,COLGIS) in university Utara Malaysia (UUM). According to Uma Sekaran (2003), the estimated number of sample (n) is based on the number of the population. As the population of this research is 20,157 thus the sample is 100.

3.4.4 Data collection

The data collection was from February 2010-April 2010. This is to be fair to all respondents to answer the questionnaires. Questionnaires were distributed by hand to the students in College of Business (COB), College of Art and Science (CAS) and College of Law, Government and international Studies (COLGIS).

3.4.5 Data Analysis

3.4.5.1 Descriptive Analysis

The aim of this analysis is to seek an understanding on the characteristics of each construct. It is utilized to illustrate frequencies, means value, and standard deviation of every research construct.

3.4.5.2 Reliability and Validity

Reliability is the extent to which measurement procedure yield the same answer however and whenever it is carried out, while validity is the extent to which it gives the correct answer (Jerome and Miller,1986).Therefore, reliability and validity of this research is very important in order to have an effective and efficient results.

3.4.5.3 Normality Test

It is one of the most assumptions made in the development of statistical procedure. it also describe the selection, design, theory and application of test for normality (Thode,2002).

Based on the analysis, the normality of the factors influencing the perception of students on ISP in UUM will be verified.

3.4.5.4 Correlation Analysis

Correlation is a vicariate measure of association (strength) of the relationship between two variables. The use of partial correlation is usually restricted to simple models of 3 or 4 variables, 5 at the most (Cohon, 1983). It was used to measure the linear relationship between multiple independent and dependent variables. The purpose of canonical analysis is to maximize the correlation between the low-dimensional projections of the two sets of variables and to explore a linear combination of one set of variables and different linear composite of another set of variables that will constitute a maximal correlation.

3.4.5.4 Regression Analysis

Regression analysis will be applied to analyze the relationships between a single dependent variable and several independent variables. The purpose of these techniques is to use independent variables, which values are known to predict the single dependent variables selected by researchers.

3.5 Summary

Hypotheses H1, H2, H3; and H4 will be tested using the analyses discussed above. Those with highest significant relationship with the ISP will be accepted and those not significant will be rejected.

CHAPTER FOUR

RESEARCH FINDINGS ANALYSIS

4.1 Introduction

This chapter results derived from data analyses and the research finding conducted in this study. Therefore, this chapter was divided into four sections. Firstly, it is showing analysis demographic variable and research constructs to identify the relationship.

Secondly, it shows factors analysis between independent variables (size of the organization, information security awareness and threat, Level of IT knowledge and business operation) and information security plan which identifies the relationship between researches constructs. Lastly, a correlations analysis between dependent and independent variables constructed to explore the direct relationship.

4.2 Descriptive Analysis

The scope of this research focuses on UUM students and students are categorized according to their colleges. Therefore, there are hundred students sampled from COB, CAS and COLGIS. Based on the data collected, the respondents are presented in summary of percentage and arranged accordingly to their colleges(refer to fig3) based on the figure 3, COB has the highest respondents of 65% followed by CAS with 30% and 5 % from COLGIS . In this research, respondents were asked about their demographic details and this is summarized in table 4 and Figure 4 below.

Colleges	Frequency	Percentage
COB	65	65.0
CAS	30	30.0
COLGIS	5	5.0
Total	100	100.0

Table 4.1 : Percentage of respondents from various colleges

4.3. Reliability test

The first research objective seeks to identify perceptional factors of information security plan. To answer this objective the reliability test will be used.

4.3.1 Information security plan reliability test

To verify the reliability of the scales summed up to measure Information security plan, Cronbach alpha value was calculated. Information security plan is a multidimensional construct of which a total of 3 items were added to measure it. The alpha value computed was 0.643, indicating the internal consistency reliability of the items measuring the underlying construct. Table 4.2 depicts the Cronbach alpha of information security plan.

Table 4.2: Information security plan

Cronbach's Alpha	N of Items
.648	3

4.3.2 Size of organization reliability

To verify the reliability of the scales summed up to measure the size of the organization, Cronbach alpha value was calculated. Size of the organization is a multidimensional construct of which a total of 2 items were added to measure it. The alpha value computed was 0.916, indicating the internal consistency reliability of the items measuring the underlying construct. Table 4.3 depicts the Cronbach alpha of the size of the organization.

Table 4.3: Size of organization reliability

Cronbach's Alpha	N of Items
.916	2

4.3.3 Information system awareness and threat reliability test

To verify the reliability of the scales summed up to measure information system awareness and threat. Cronbach alpha value was calculated. Information system development is a multidimensional construct of which a total 3 items were added to measure it. The alpha value computed was 0.648, indicating the internal consistency reliability of the items measuring the underlying construct. Table 4.4 depicts the Cronbach alpha of information system development.

Table 4.4: information system awareness and threat reliability

Cronbach's Alpha	N of Items
.648	3

4.3.4 Level of Information technology knowledge reliability test

To verify the reliability of the scales summed up to measure the level of information technology knowledge, Cronbach alpha value was calculated. The level of information technology knowledge is a multidimensional construct of which a total 5 items were added to measure it. The alpha value computed was 0.806, indicating the internal consistency reliability of the items measuring the underlying construct. Table 4.5 depicts the Cronbach alpha of the level of information technology knowledge.

Table 4.5: Level of Information technology knowledge reliability

Cronbach's Alpha	N of Items
.806	5

4.3.5 Business operation reliability test

To verify the reliability of the scales summed up to measure business operation, Cronbach alpha value was calculated. Business operation is a multidimensional construct of which a total 5 items were added to measure it. The alpha value computed was 0.856, indicating the internal consistency reliability of the items measuring the underlying construct. Table 4.6 depicts the Cronbach alpha of business operation.

Table 4.6: Business operation reliability test

Cronbach's Alpha	N of Items
.856	5

4.4 Correlation

Correlation is a vicariate measure of association (strength) of the relationship between two variables. It varies from 0 (random relationship) to 1 (perfect linear relationship) or -1 (perfect negative linear relationship). It is usually reported in terms of its square, interpreted as percent of variance explained. The use of partial correlation is usually restricted to simple models of 3 or 4 variables, 5 at the most (Cohon, 1983).

Correlation will also be attenuated to the extent there is measurement error, including use of sub-interval data or artificial truncation of the range of the data. Correlation can also be a misleading average if the relationship varies depending on the value of the independent variables.

Table 4.7 : Correlations of ISP with the independent variables

		Informati0n security plan	size of organizati on	informatio n security awareness and threat	Level of information technology knowledge	business operation
information security plan	Pearson Correlation	1	.344(**)	.693(**)	.906(**)	.573(**)
	Sig. (2-tailed)	.	.000	.000	.000	.000
	N	100	100	100	100	100
size of org	Pearson Correlation	.344(**)	1	.499(**)	.283(**)	.171
	Sig. (2-tailed)	.000	.	.000	.004	.089
	N	100	100	100	100	100
information system development	Pearson Correlation	.693(**)	.499(**)	1	.526(**)	.538(**)
	Sig. (2-tailed)	.000	.000	.	.000	.000
	N	100	100	100	100	100
information technology	Pearson Correlation	.906(**)	.283(**)	.526(**)	1	.569(**)
	Sig. (2-tailed)	.000	.004	.000	.	.000
	N	100	100	100	100	100
business operation	Pearson Correlation	.573(**)	.171	.538(**)	.569(**)	1
	Sig. (2-tailed)	.000	.089	.000	.000	.
	N	100	100	100	100	100

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

* Correlation is significant at the 0.05 level (2- tailed).

Table 4.8: The summary of Correlation of ISP with the independent Variables

Correlation	Size of organization	Information security awareness and threat	Level of IT knowledge	Business operation
Information security plan	.344(**)	.693(**)	.906(**)	.573(**)
Sig.(2-tailed)	.000	.000	.000	.000
N	100	100	100	100

A high correlation (whether negative or positive) points to a strong relationship between the variables, while a low correlation coefficient (r) indicates a weak relationship. Cohen (1988) provides a classification of the strength of relationship based on the size of the value of Pearson Correlation coefficient (r) thus:

Table 4.9 Guideline for Pearson correlation strength

r =.10 to .29 or r = -.10 to -.29	Small
r = .30 to .49 or r = -.30 to -.49	Medium
r = .50 to 1.0 or r = -.50 to -1.0	Large

Therefore, from the table above (Table 4.9), all the independent variables correlate with the dependent variable. Level of IT knowledge had the highest correlation ($r = .906$ where $p < 0.05$), followed by information security awareness and threat ($r = .693$ where $p < 0.05$), business operation ($r = .573$ where $p < 0.05$) and size of organization ($r = .344$ where $p < 0.05$) had a medium influence on ISP. Overall, all the independent factors positively influence the dependent variable (ISP).

4.5 Multiple Regression Analysis

4.5.1 Research objective 2

The second objective is to develop a framework based on the identified perceptional factors of information security plan. To answer this objective the multiple regression analysis will be utilized. Specifically, the Beta coefficient table (Table 4.10) will be used.

Table 4.10: The model summary (d)

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.941(a)	.886	.881	.61815
2	.941(b)	.886	.882	.61619
3	.941(c)	.885	.883	.61415

A Predictors: (Constant), business operation, size of organization, level of information technology knowledge, information security awareness and threat.

B Predictors: (Constant), size of organization, level of information technology, information security awareness and threat

C Predictors: (Constant), level of information technology, information security awareness and threat

D Dependent Variable: information security plan.

Table 4.10 above (model summary) shows the value of R Square and the Adjusted R Square value. The R^2 value tells us the amount of variance in the dependent variable (Information security plan) accounted by the model. A high variance indicates a high level of success of the model. Sometimes, the R square value have a propensity to somewhat overrate the success of the model when applied to the real world scenario. The Adjusted R Square value provides a more correct estimate measure of the success of the model. In my own case, the R Square value for the first model (1) is .886 and an adjusted R square of .881, then the second model (2) has an R square of .886 and an adjusted R square is .882. The last model (3) consists of the most significant independent variables (i.e. level of IT knowledge & information security awareness and threat) with an R square value of .885 and an Adjusted R Square of .883. To better depict a true estimate the Adjusted R Square indicates that the model explains 88.3% of the variance in the dependent variable. Overall, all three models are deemed to be good for their predictive power is very high (above 80%).

Table 4.11: The Coefficients (a)

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	.261	.681		.383	.703
	size of org	-.037	.054	-.028	-.687	.494
	information system awareness and threat	.161	.024	.322	6.638	.000
	information technology	.461	.027	.760	17.063	.000
	business operation	-.013	.021	-.028	-.627	.532
2	(Constant)	.214	.675		.317	.752
	size of org	-.032	.054	-.024	-.597	.552
	information system awareness and threat	.155	.022	.311	6.922	.000
	information technology	.454	.025	.749	18.456	.000
3	(Constant)	-.096	.430		-.224	.824
	information system awareness and threat	.150	.020	.299	7.405	.000
	information technology	.454	.025	.748	18.508	.000

A. Dependent Variable: information security plan

From the table (Table 4.11) presents the Standardized Beta Coefficient. This value tells us the unique contribution of each independent variable to the model when other predictor variables are controlled for. A large value implies that the underlying variable made a significant contribution to the model. Considering the Standardized Beta column, we can see that only three variables; level of IT knowledge (Beta= .760), ISA (Beta= .748) and Business operation (749) made

significant contribution to the model while size of the organization has low significant. Overall, level of information technology made the largest contribution in explaining the dependent variable. Therefore, from the table above, Beta is high with 322 and 760 while significant is low with 000 and 000 .Although, the level of IT is higher than information system development. The result shows that both have a greater impact on information security plan. The results obtained in the multiple regression analysis, the level of information technology, information security awareness and threat and business operation are significant. They explain 88.3.% of the variance in the dependent variable (ISP). Only two of the independent variables (i.e level of IT knowledge & information security awareness & threat) were found to have the largest contribution to the model (Beta = .748 where p = .000 and Beta =.299 where p is = .000 respectively). The table below (Table 4.12) shows the ANOVA which evaluates the statistical significance of the model. The result shows that the research model is significant (Sig. =.000, meaning that p<.005).

Table 4.12: ANOVA (d)

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	282.660	4	70.665	184.936	.000(a)
	Residual	36.300	95	.382		
	Total	318.960	99			
2	Regression	282.510	3	94.170	248.017	.000(b)
	Residual	36.450	96	.380		
	Total	318.960	99			
3	Regression	282.374	2	141.187	374.328	.000(c)
	Residual	36.586	97	.377		
	Total	318.960	99			

a Predictors: (Constant), business operation, size of organization, level of information technology, information security awareness and threat.

b Predictors: (Constant), size of organization, level of information technology, information security awareness and threat.

c Predictors: (Constant), level of information technology, information security awareness and threat.

d Dependent Variable: information security plan.

4.6 Summary of Hypotheses Tested

Table 4.13: Summary of hypotheses tested

Hypotheses Tested	Status
H1. Size of the Organization	Rejected
H2. Information security awareness and threat.	Accepted
H3 Level of IT Knowledge	Accepted
H4 Business Operation	Rejected

Based on the analysis performed, two of the variables are found to be significant.(H2,H3), while the remaining two(H1& H4) were not significant. The variables that were significant were accepted and those that were not significant were rejected.

4.7 SUMMARY

Data collected was analyzed and interpreted in a series of stages. Firstly, the demographic profile of respondents was summarized and analyzed. Secondly, the reliability of the items used in measuring the constructs was validated using Cronbach's alpha.

Thirdly, the correlation of the dependent variables and the dependent variable was ascertained through Pearson product moment correlation method.

And lastly, standard multiple regression analysis was used to establish the statistical significance of the model and the predictive power of each independent variable in explaining the dependent variable (information security plan)

CHAPTER 5

DISCUSSION, CONCLUSION AND FUTURE WORKS

5.1 Discussion

The last chapter contains discussion conclusion and future works of the research project. The UUM students were investigated during the course of this study using questionnaire survey. The variables that were used in present work includes size of the organization, information security awareness and threat, level of IT knowledge; and business operation. The respondents of this questionnaires survey were about 91.99 percent. Therefore, descriptive analysis, reliability test, correlation and regression analysis were used.

The reliability test found that all variables are reliable. The Factor tables showed that all variables are significantly related and correlation analysis indicated that the independent variables are significantly having relationship with the dependent variables.

The results of the correlation analysis showed that all the independent variables have impact (ISP).The level of IT knowledge had the highest correlation with the ISP because a high correlation (whether negative or positive) points to a strong relationship between the variables, while a low (small) correlation coefficient (r) indicates a weak relationship Cohen (1988). Level of IT knowledge had the highest correlation ($r = .906$ where $p < 0.05$).

Multiple regression analysis indicated that only two among the four factors advanced before and had a significant influence on (ISP). For instance, only two of the independent variables (i.e level of IT knowledge & information security awareness & threat) were found to have the largest contribution to the model (Beta = .748 where p = .000 and Beta =.299 where p is = .000 respectively). But level of IT knowledge impact most on ISP.

By and large, most of the respondents agree that the variables especially mentioned above are the factors influencing ISP in UUM. It is very important that the discussion concluded that even though the size of the organization has medium significant relationship.. However, the three independent variables significantly have relationship with dependent variables that support the research hypotheses, in chapter three which had been discussed earlier in the study.

5.2 Conclusion

Through the literature review, it is very succinct that information security plan is very imperative to the organization. Therefore, the researcher has succeeded in achieving the objectives set earlier.

The objectives to identify perceptional factors of information security plan, developing a framework based on the identified perceptional factors of information security plan and validating the framework from the perspective of UUM has been achieved because there is a significant correlation between dependent variable and independent variables. Therefore, an information security plan will improve and bring about effectiveness. Furtherance of application of information security plan will save the organization and increase information security efficiency. The finding shows that in general, UUM students share the same perception that information security plan is very much vital in an organization especially in an educational institution like UUM.

5.3 FUTURE WORKS

This research should be extended to broader the perspectives of seeing an information security plan as important which need to be implemented. Hence, this research could certainly be extended to include management staffs and organization as a whole.

BIBLIOGRAPHY

Anderson J 1993 Why Crypto system fails, Communication of the ACM, Vol 37 No 11 Pg 32-34.

Aiponey M.T (2001) five dimension of information Security Awareness Computers & Society Cyber thesis.

Andress,M (2001).Surviving security. How to integrate people, process and technology, Indianapolis: Sams Publishing PP40-58.

Baltzan /Philips et al (2008) "Business driven information System Second Edition".

BS 7799-1(1999), Information Security Management Part 1.Code of Practice for information security Management, British Standard Institution, London.

Dr. Somnath Bhattacharya, (June 30, 2006) Florida Atlantic University (sbhatt@fau, edu)" is there a relationship between firm, Corporate Governance, and a firm's decision to form a technology Committee"

Dr. Noor Azizi Ismail (2008) Faculty of Accountancy, College of Business, Universiti Utara Malaysia."Information technology governance, Funding and structure".

Information Reading Room. SANS Institute.

Lawrence D. Brown J. Mack Robinson Distinguished Professor of Accountancy Georgia University (December 7, 2004) "Corporate Governance and Firm Performance."

Marcus L. Caylor (December 7,2004)PhD Candidate Georgia University December 2004 "Corporate Governance and Firm Performance."

NIST Special Publication 800-16 (1998, Information Technology security Training Requirements: role and Performance Based Model.

Omar Bin Zakaria (2007) Investigating information security culture challenges in a public sector organization: a Malaysian case

Ronald F. Premuroso,(June30 ,2006) Florida Atlantic University (premuros@fau.edu)"is there a relationship between firm, Corporate Governance ,and a firm's decision to form a technology Committee"

Russell,C (2002),security Awareness- implementing effective Strategy.

Selamat,MH,Suhaimi,M,(1990),"Strategic Information Systems planning and Strategic information security planning implementation in Malaysia government agencies, Procedure of international conference on ICT for the Muslim World, Kuala Lumpur.

Siponen M.T (2000) On the role of human morality in information system security.

Security information Resources Management journal Volume No4 PP15-33.

Spurlling, P(1995) Promoting security awareness and commitment, information management and computer security .Volume 3.No 2 PP,20-26.

Thomason, M.E and Von Solme,R (1997).An effective information Security awareness Program for industry. proceeding of the WG 11.2 and WG11.1 of the TC111F1.

University of California Berkeley,(2006),information Technology at UC Berkeley: Governance, structure and funding. Final report and recommendation. Available at http://technology.berkeley.edu/pdf/IT_Report.pdf(accessed 30 November, 2006).

Jerome Kirk and Miller, (1986) Reliability and Validity in Qualitative Research.

Henry C.Thode, (2002) Testing for Normality.

APPENDICES

APPENDIX A:

SAMPLE OF QUESTIONNAIRES

Information Security Plan Evaluation Questionnaires used in this Research

Objectives

This project is being conducted by principle researcher Babatunde Dorcas Adebola of College of Business, Universiti Utara Malaysia.

The purpose of this study is to identify the factors that may influence students' perception on information security plan in Universiti Utara Malaysia. Factors influencing students' views will be investigated from various colleges within the Universiti including College of Art and science, College of Business and college of law and government.

Process

The data will be collected via a questionnaire that will take approximately 5 to 10minutes to complete. The researchers will request participants to answer several questions.

Confidentiality

The research is based on information system security plan rather than the individual. Therefore, all information supplied will be treated with the utmost confidence. Results will always be reported in such a way that anonymity of the participants is preserved.

Consent and Feedback

Participation in the study is entirely voluntary and withdrawal from the study is allowable at any time. The overall results of this study will be made available on requests to any participant.

Thank you for your cooperation and participation.

Babatunde Dorcas Adebola

College of Business

Universiti Utara Malaysia
06010 Sintok-Kedah, Malaysia.

Email: adebola4mine@yahoo.com

Tel No: 0194345942.

Supervisor: Dr. Mohamad Hisyam Selamat

College of Business

Universiti Utara Malaysia

Email: hisyam@uum.edu.my

Demographic Information

Please answer or tick one of the following boxes for each question.

1. What is the name of your University and in which college are you currently studying

College..... or Department .....

2. Your current student status and in what year at university are you studying? (Please tick):

- ❑ Undergraduate
- ❑ Graduate

Current year of study? .....year

3. In what main subject areas are you currently majoring? (Please tick):

- ❑ Accounting
- ❑ Business Administration
- ❑ Finance and Banking
- ❑ Economics
- ❑ International Business
- ❑ Management
- ❑ Marketing
- ❑ Technology Management
- ❑ Not Decided yet
- ❑ Others (Please describe if you choose this option .....)

4. What is your age? .....

5. What is your gender?

- ☐ Male
- ☐ Female

6. If you currently have or have had paid employment, what kind of job was it / is it?

- ☐ No paid job (includes full-time students)
- ☐ Unskilled or semi-skilled manual worker
- ☐ General trained office worker or secretary
- ☐ Vocationally trained craftsperson, technician, nurse, artist or equivalent
- ☐ Academically trained professional or equivalent (but not a manager of people)
- ☐ Manager of one or more subordinates (non-managers)
- ☐ Manager of one or more other managers

7. What is your nationality? .....

8. How important are each of the following factors to you when considering information security system? (please circle only one response for each question):

	FACTORS	Not Importance	Less Importance	Indifference	Important	Very Important
a	**Number of Students**	1	2	3	4	5
b	infrastructure	1	2	3	4	5
c	**Number of Student intake**	1	2	3	4	5
d	Awareness of information security	1	2	3	4	5

e	Educating and rewarding users on security awareness is a great way to build conscious environment	1	2	3	4	5
f	Security of student's information	1	2	3	4	5
g	Information security plan lowers risk of being hacked	1	2	3	4	5
h	Level of concern for data secrecy and theft	1	2	3	4	5
i	Level of IT knowledge is important in security plan.	1	2	3	4	5

j	Vulnerability to information	1	2	3	4	5
k	Confidentiality of data	1	2	3	4	5
l	Availability of information	1	2	3	4	5
m	Protection of data against natural disasters	1	2	3	4	5
n	Security of academic's information	1	2	3	4	5
o	Interaction with others	1	2	3	4	5
p	Length of work hours	1	2	3	4	5
q	Sufficient time for your personal or family life	1	2	3	4	5
r	Good physical working conditions (good ventilation and lighting,	1	2	3	4	5

	adequate space)					
s	How do you view ISP in UUM	1	2	3	4	5
t	What can you say about the significant of ISP in UUM	1	2	3	4	5
u	The level of ISP in UUM	1	2	3	4	5

THE END

Thank you for your cooperation.

Appendix B:

Information Security Plan Template

1. **Information security Plan Name/Title:** Unique identifier and name given to the system.

2. **Information Security Owner and other Designated Contacts:** Name, title, agency, address, email address, and phone number of person who owns the system.

3. **Authorizing Official:** Name, title, agency, address, email address, and phone number of the official designated as the authorizing official, such as Agency Head or designated ISO.

4. **Information Security Operational Status:** Indicate the operational status of the system. If more than one status is selected, list which part of the system is covered under each status.

Operational	Under Development	Major Modification

5. **General System Description/Purpose:** Describe the function or purpose of the system and the information processes.

6. **System Environment:** Provide a general description of the technical system. Include the primary hardware, software, and communications equipment.

7. **Related Laws/Regulations/Policies:** List any laws or regulations that establish specific requirements for the confidentiality, integrity, or availability of the data in the system.

8. Plan to Implement Recommended Controls (reference Risk Assessment): Provide a description of how security controls recommended from the risk assessment are being implemented or planned to be implemented, and who is responsible for the implementation.

9. Information Security Plan Completion Date: _____ Enter the completion date of the plan.

10. Information Security Plan Approval Date: _____ Enter the date the system security plan was approved and indicate if the approval documentation is attached or on file.

Appendix C:

Correlation table

Table 5: The Correlations of ISP with independent variables

		information security plan	size of organization	information security awareness and threat	Level of IT knowledge	business operation
information security plan	Pearson Correlation	1	.344(**)	.693(**)	.906(**)	.573(**)
	Sig. (2-tailed)	.	.000	.000	.000	.000
	N	100	100	100	100	100
size of organization	Pearson Correlation	.344(**)	1	.499(**)	.283(**)	.171
	Sig. (2-tailed)	.000	.	.000	.004	.089
	N	100	100	100	100	100
Information system development.	Pearson Correlation	.693(**)	.499(**)	1	.526(**)	.538(**)
	Sig. (2-tailed)	.000	.000	.	.000	.000
	N	100	100	100	100	100
information technology	Pearson Correlation	.906(**)	.283(**)	.526(**)	1	.569(**)
	Sig. (2-tailed)	.000	.004	.000	.	.000
	N	100	100	100	100	100
business operation	Pearson Correlation	.573(**)	.171	.538(**)	.569(**)	1
	Sig. (2-tailed)	.000	.089	.000	.000	.
	N	100	100	100	100	100

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

* Correlation is significant at the 0.05 level (2-tailed).

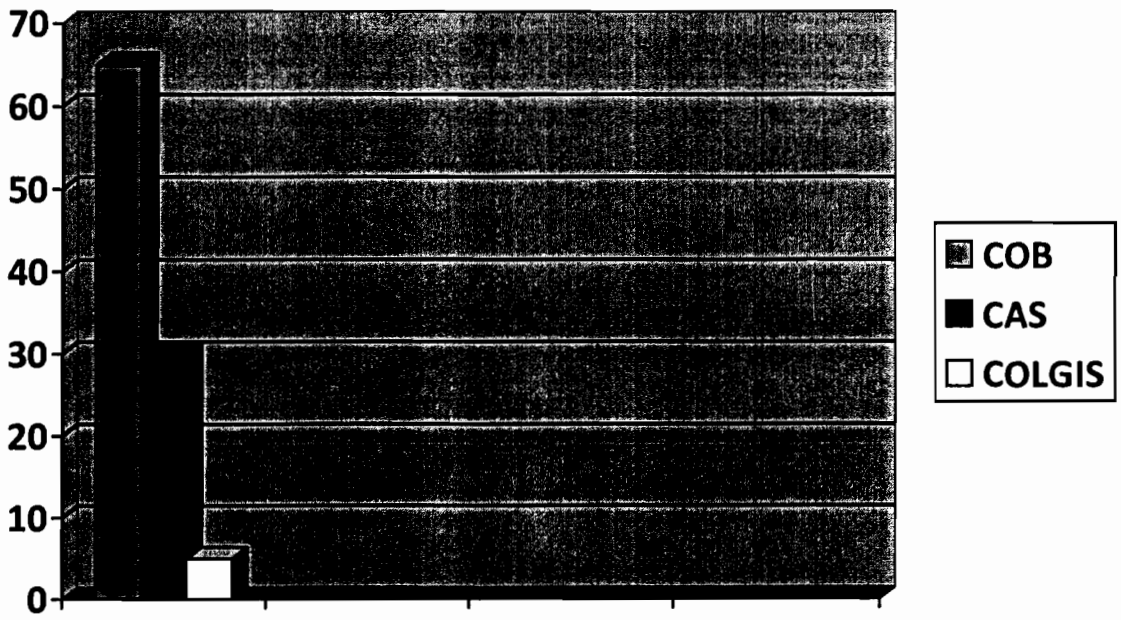

Figure 3.1: Percentage of respondent from various colleges

LIST OF FIGURES

LIST OF TABLES