ASSESSMENT OF EMPLOYEE'S KNOWLEDGE AND COMPLIANCE ON INFORMATION SECURITY GOVERNANCE

CHOW WIN NIY

MASTER OF BUSINESS ADMINISTRATION
(CORPORATE GOVERNANCE)

UNIVERSITI TUNKU ABDUL RAHMAN

FACULTY OF ACCOUNTANCY AND MANAGEMENT

MARCH 2014

Assessment of Employee's Knowledge and Compliance on Information Security Governance

Chow Win Niy

A research project submitted in partial fulfillment of the requirement for the degree of

Master of Business Administration

(Corporate Governance)

Universiti Tunku Abdul Rahman

Faculty of Accountancy and Management

March 2014

Assessment of Employee's Knowledge and Compliance on Information Security Governance

By

Chow Win Niy

This research project is supervised by:

Dr. Hen Kai Wah

Senior Lecturer

Department of International Business

Faculty of Accountancy and Management

DECLARATION

I hereby declare that:

(1) This MKMB25106 Research Project is the end result of my own work and that due acknowledgement has been given in the references to all sources of information be they printed, electronic, or personal.

(2) No portion of this research project has been submitted in support of any application for any other degree or qualification of this or any other university, or other institutes of learning.

(3) The word count of this research report is 16,359.

Name of Student: CHOW WIN NIY

Student ID: 10UKM06609

Signature: *Win Niy*

Date: 3rd March 2014

ACKNOWLEDGEMENT

I would like to express the deepest appreciate to Dr. Hen Kai Wah for his time and excellent guidance throughout this study being carried. His encouragements always motivate me to complete in this research project.

Next, to all my family members who always try their best in helping me to take care my son, Zi Yu and daughter, Zi Xuan especially my lovely husband, Wong Chee Hoe (Jeff) and dearest parents, Chow Chee Chiang (David) and Lee Mooi @ Lee Moi. With their lovely care on my children, I can concentrate while attending the classes and complete this Master of Business Administration (MBA) course and research project.

Special thanks to respondents who had participate in the research study and thus ensured the success thereof. Last but not least, lecturers and staffs from University Tunku Abdul Rahman (UTAR) for getting me the opportunity to further my study and assist me along the journey of my MBA study.

DEDICATION

To my lovely husband, Wong Chee Hoe (Jeff), thanks for his fully supports and understanding during the completion of this research study.

To my dearest parents, Chow Chee Chiang (David) and Lee Mooi @ Lee Moi, thanks for their unlimited support throughout my life and instilled qualities in me that enable me to complete this study.

TABLE OF CONTENTS

Page

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

This research study reviewed relative literature on Internet and information security governance within organisations to determine what factors affecting employees' compliance on information security governance. Five key factors were determined to potentially affecting employees' compliance based on this literature review. A survey instrument was designed to determine if each of the key factors had a significant association with the compliance on information security governance, assess the knowledge of employees on information security governance and employees' perception towards information security governance after survey done. Results show that the only key factors which affect the compliances are education and training and privacy. Employee awareness has no significant relationship toward employees' compliance on information security governance.

CHAPTER 1

INTRODUCTION

1.1 Overview

Chapter 1 discusses the research's background whereby the researcher try to answer the questions of "what is information security governance?" and "why is information security governance necessary?". It formed the base of this study which assessing the employee's knowledge and compliance on information security governance. Next, problem statement was clarified.

Significant of this study accordance to individual level, body of knowledge and organisation level was presented and four research questions had been clearly listed before the research objectives being derived. Consequently, the scope of this study being discussed. At the end of this chapter, researcher proposed remainder chapters and a summary was written.

1.2 Background to Research

"Information security provides the management processes, technology and assurance to allow business management to ensure business transactions can be trusted; ensure information technology services are usable and can appropriately resist and recover from failures due to error, deliberate attacks or disaster; and ensure critical confidential information is withheld from those who should not have access to it" (COBIT Security, 2004).

As quoted in ISO 17799 (2005), information is an important asset to business. It is present in many forms (voice recording, paper, electronic documents and others) and stored in various ways (electronic database, hard copy files, back ups and archive) which enable organisation transmit electronically or by post and even as films and short message services (SMS).

Since information treated and recognised as an asset to organisations, it should be protected as with other business assets to ensure that information is available and confidential and that its integrity is preserved where necessary (ISO 17799, 2005). Consequently, information security governance is recognised as part of the component of corporate governance for all organisations. It is a must for organisations to develop and implement the information security governance within the organisation.

A comprehensive information security governance must be able to suit and align with organisation's goals or missions and operations. Various of information security governance being introduced to managers and IT professionals. For example, internationally, those common and comprehensive information security governance are refer to Control Objectives for Information and Related Technology (COBIT), Information Technology Infrastructure Library (ITIL), International Standard Organisations 17799 (ISO 17799) which will be further discussed in later chapters. As in Malaysia, Cyber Laws of Malaysia had been in force in the year of 1998 which focuses more on the technology security systems.

In view of data or information protection, Personal Data Protection Act 2010 just comes into effect recently.

Tremendous develop in technology not only enhancing employees in daily works but also giving criminals to exploit organisations information assets. In such, it is important for employees to comply with the organisation's information security governance. In worst, some employees might not even being introduced to the term of information security governance once they were being recruited.

According to McIlwraith (2006), organisation's annual profit is potentially lost due to information security incidents whereby it is found that up to 80% of such information security incidents were caused by employees. Meanwhile, PriceWaterhouseCoopers had conduct a survey with the conclusion stated that "human error rather than technology is the root cause of most security breaches" (PWC 2004).

In view of the past study findings, it is relatively important for employees to understand the importance of what, when and how to protect the organisation's information assets. Employees should know and clear about the circumstances of not to comply with the information security governance.

1.3Problem Statement

It was found that most of the researches were focused into the introduction, development and also implementation of information security governance (Avison, 1993; Brown & Magill, 1994; Hirschheim, Schwarz & Tood, 2006). Those researches were useful as the guidance for organisations to build and form their own information security governance as to comply with the requisition and it was just a starting point.

Further, most of the recommendations were suggest that employee's awareness should be created in order to get them comply with the information security governance in organisation. However, researcher believes that employee awareness is not the only factor and it is not necessary correlate to the compliances on organisation's information security governance.

Since there were lots of researches being done in-depth of developing and implementing, researcher believes that awareness level among employees especially those at management level had been exposed to information security governance. Thus, researcher would like to examine the current knowledge of employees toward information security governance since employees had been exposed to it for such a long time frame.

Thus, this study had been carried to assess the employee's knowledge and compliances on information security governance in Malaysia context. More factors had been included to test against the significant relationship with employee's compliances. Lastly, opinion of participants about information security governance was asked at the end of the survey.

1.4 Significant of the Study

1.4.1 Individual Level

Most of the employees might know and involved in information security governance. But most of the employees are only theoretically complying and not fully in practice. Information security is a process of keeping the information in secure. Thus, it is highly correlated to employees' daily working.

Throughout this survey, participants (or employees) will have better understanding about their current knowledge level about information security

governance. Coincidently, this study could raise employees' awareness in their current compliances on information security governance in organisation.

1.4.2 Body of Knowledge

Most of the previous research studies found were focus in the field of assessing the awareness in information security governance or development of successful information security governance framework and mainly aim for management level participants. Contrary, this study is aim to focus on employee's knowledge and compliances on information security governance in Malaysia context.

As quantitative research, this study may lay a foundation for further work that could show a more direct relationship between the factors and compliances of employees in information security governance. Beside, it could indicate a correlation between these factors and an increase in the success of compliance on information security governance.

1.4.3 Organisational Level

Managers and IT professional able to cultivate a better and comprehensive information security governance framework by understood employee's perception and factors that influence their compliances toward information security governance. Previously, managers and IT professional were instructed to develop but not emphasize to implement the information security governance in organisations. As the result, information security governance will just design as a handbook to employees and being display to show that organisation is complying with the requirement of corporate governance.

Without proper implementation and compliances, organisations information assets are still threatened by various risks and threats. Consequently, this will lead to unsecure of organisational information assets and unlimited lost. Therefore, methods or frameworks could be proposed and tested for improving organisational information security governance by knowing the factors that influence employee's compliance.

1.5 Research Question

Research questions were formed and listed as below:

1. What are the employee's perceptions in information security governance?
2. What are the key factors that might affect the compliances on information security governance of employees in Malaysia?
3. What are the opinions of employees upon completing the survey about information security governance?
4. Are there any differences between gender toward perceptions in information security governance, compliances and opinion upon completing the survey?

1.6 Objectives of the Study

1. To assess the perception of employees in information security governance.
2. To examine the key factors that affect employees' compliance on information security governance.
3. To assess the employees' opinions on information security governance after survey done.

4. To determine whether there is any differences among gender on perception in information security governance, compliances and opinion upon completing the survey.

1.7 Scope of the Study

The targeted respondents for this study were employees in Malaysia. All assessment questions are related to information security governance. This study aims to assess employee's knowledge and perception about self knowledge in information security governance at the end of this survey. Apparently, the main focus will be to examine the factors which influence the compliance of employee in security governance.

This study was not specific drawn out the targeted respondents of managerial group or IT professionals. The logical behind is sustainable information security governance should comply by all the members or employees in the organisation. A survey instrument will be uploaded and sent through online to those who were available and easy to reach by researcher.

1.8 Organisation of the Report

The report of this study is structured into five chapters. Each of the five chapters started with an overview as briefly describe the contents in the particular chapter and ended up with a summary for the contents in that chapter.

Chapter 1 "Introduction", which presents the background of study, problem statement, significant of the study at individual, body of knowledge and organisation level, research questions, research objectives, scope of the study and organisation of the report.

Chapter 2 “Literature Review”, which comprises a comprehensive literature review in information security and the five factors being studied.

Chapter 3 “Methodology”, which discuss on the research design, development of survey instrument, reliability and validity test, data collection, population and sampling, data coding, data analysis method and ethical consideration.

Chapter 4 “Research Results and Interpretation”, which present the details of analysis and results generated from this research study’s data through SPSS software.

Chapter 5 “Discussion and Conclusion”, which summarise the results of study, drawn out the conclusion for this research study and provides some recommendations for further research.

1.9 Summary

Information security governance has be included as part of corporate governance for all the organisations around the world. Management could refer to some of the common information security governance in order for them to develop a comprehensive information security framework which is sustainable and best fit into organisation’s goals, mission and operations. Existing framework such as COBIT, ITIL and ISO17799 could be the model framework for most of the organisation. In Malaysia, several acts had been enforcing such as Cyber Laws of Malaysia and Personal Data Protection Act 2010 in order to protect the organisation’s information assets.

Throughout this study, employees being explore to information security governance. As a quantitative research, this study may lay a foundation in future research work as to examine the factors related to compliances on information

security governance. In organisation level, management or IT professionals could review and examine their existing information security framework by taking this study results into consideration.

Research questions and objectives further describe the aim and focus of this study. However, the results found or conclusion made in this study does not fully represent the trend or perception of all employees in Malaysia. It was due to the limited scope as stated in this chapter. The organisation of the report for this study had been stated at the end of Chapter 1 as to get readers a reference on the remainders contents in this study report.

CHAPTER 2

LITERATURE REVIEW

2.1 Overview

In Chapter 2, literature was critical reviewed by the researcher. This chapter is started with a brief history of Internet as when it began. Continually, the finding of Asia Internet usage was presented and interpreted with the focus on Malaysia's statistical figure. Phishing issues and information security governance being further explored and discussed in the following chapters.

Different type of information security governance had been introduced by the researcher and this study was extended into the field of compliance for information security governance. This will be the main focus and aim for this study whereas 5 factors which going to be tested against the compliance were further discussed in Chapter 2. After all, theoretical framework and conceptual

framework was draw as a mapping for readers. At the end of this Chapter 2, hypotheses were stated which tends to achieve by the researchers in this study.

2.2 Internet

The history of the Internet began with the development of electronic computers in the 1950s. Variety of protocols were developed and used for internetworking in which multiple separate networks could be joined together into a network of networks. The Internet protocol suite (TCP/IP) was standardized in year 1982. Consequently, the Internet was introduced as concept of a world-wide network of interconnected TCP/IP networks (www.computerhistory.org).

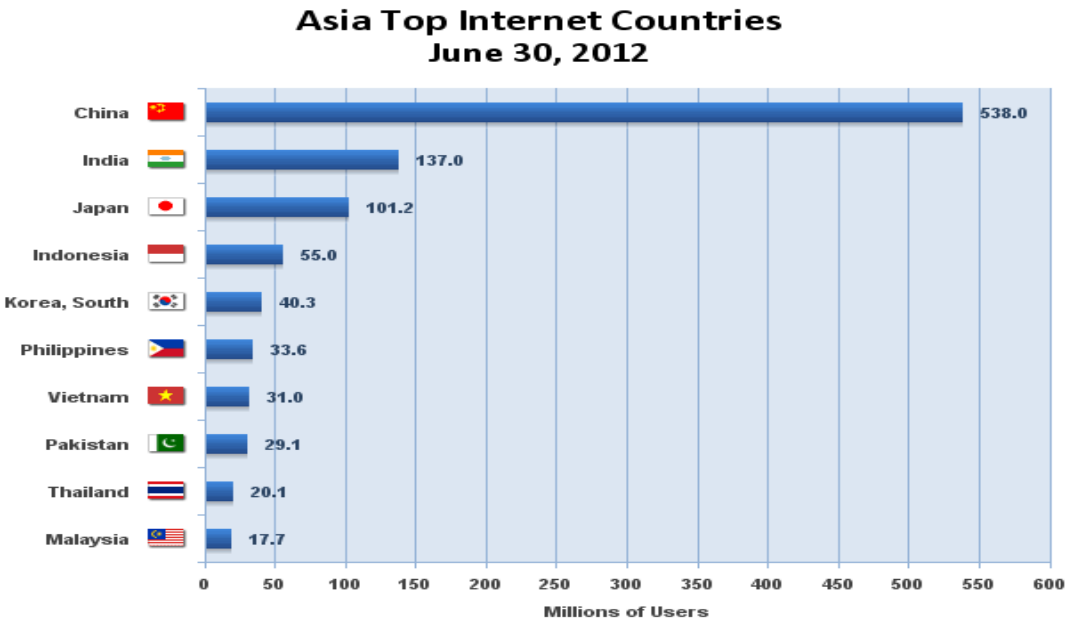
Back to 1980s, the increased use of personal computers made the issue of information security even more important, as personal computers were integrated into local area networks and small networks became connected to larger corporate networks and the Internet. In 1990s, user-friendly network utilities, and easy access to Internet resources, novice operators were able to access information from around the world as technology improved through the use of graphical web browsers, graphical user interfaces for operating systems. In other words, the distance between users around the world had been indirectly shortened.

The Internet today is a widespread information infrastructure and its influence reaches not only to the technical fields of computer communications but throughout society as we move toward increasing use of online tools to accomplish electronic commerce, information acquisition, and community operations. These advances also give criminals the necessary tools, opportunity, and experience to exploit users and networks.

2.2.1 Internet Usage in Malaysia

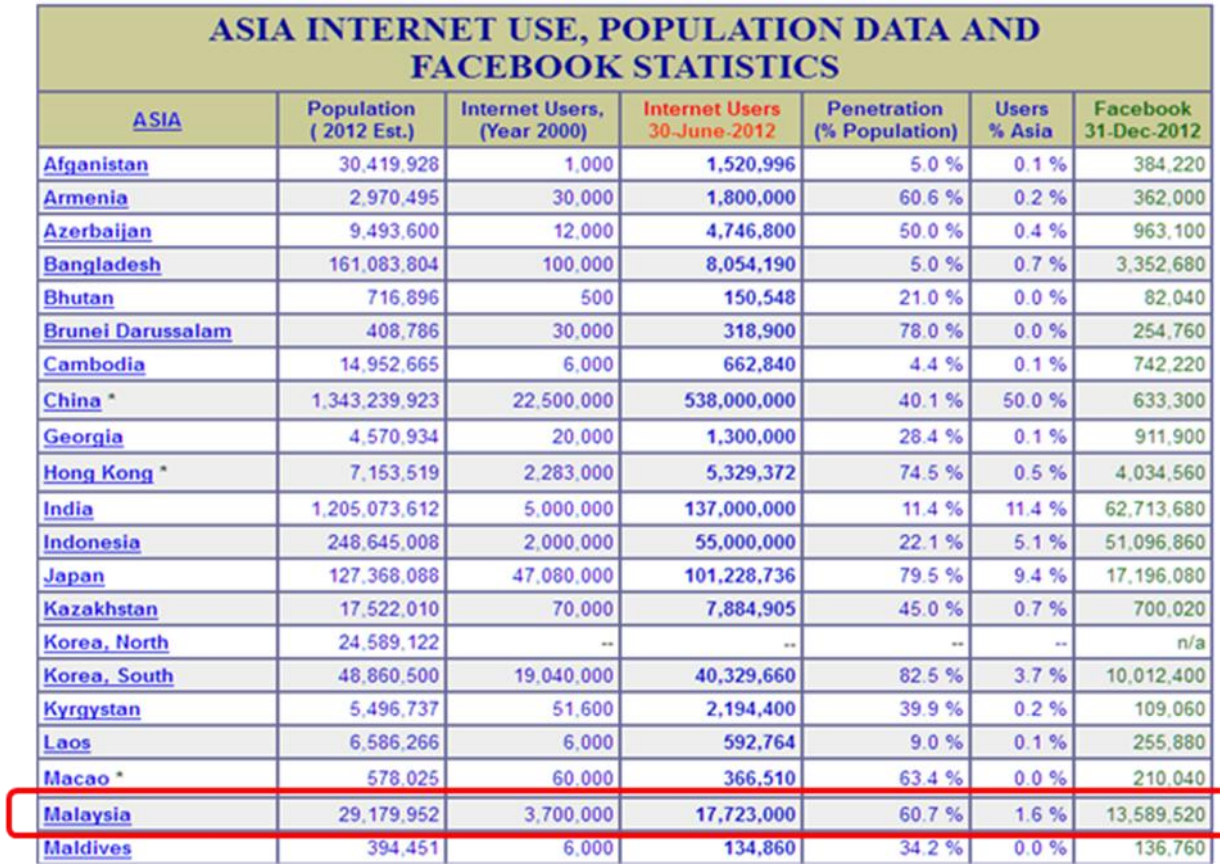
According to the statistical report as at 30th June 2012 by Internet World Stats, Malaysia was one of the top ten countries in Asia top internet countries statistical board (Figure 1). There were total of 17,723,000 Internet users in Malaysia which contributed 1.6% in the Asia Internet user statistic as highlighted in Figure 2. Beside, Malaysia's Internet penetration percentage was ranked 8th with just right behind of South of Korea (82.5%), Japan (79.5%), Brunei (78.0%), Taiwan (75.4%), Singapore (75%), Hong Kong (74.5%), and Macau (63.4%).

Figure 1: Asia top Internet countries



Note: Adopted from *Internet Usage in Asia.* Retrieved February 10, from http://www.internetworldstats.com/stats3.htm

Figure 2: Asia Internet use, population data and Facebook statistics



ASIA INTERNET USE, POPULATION DATA AND FACEBOOK STATISTICS

ASIA	Population (2012 Est.)	Internet Users, (Year 2000)	Internet Users 30-June-2012	Penetration (% Population)	Users % Asia	Facebook 31-Dec-2012
Afganistan	30,419,928	1,000	1,520,996	5.0 %	0.1 %	384,220
Armenia	2,970,495	30,000	1,800,000	60.6 %	0.2 %	362,000
Azerbaijan	9,493,600	12,000	4,746,800	50.0 %	0.4 %	963,100
Bangladesh	161,083,804	100,000	8,054,190	5.0 %	0.7 %	3,352,680
Bhutan	716,896	500	150,548	21.0 %	0.0 %	82,040
Brunei Darussalam	408,786	30,000	318,900	78.0 %	0.0 %	254,760
Cambodia	14,952,665	6,000	662,840	4.4 %	0.1 %	742,220
China *	1,343,239,923	22,500,000	538,000,000	40.1 %	50.0 %	633,300
Georgia	4,570,934	20,000	1,300,000	28.4 %	0.1 %	911,900
Hong Kong *	7,153,519	2,283,000	5,329,372	74.5 %	0.5 %	4,034,560
India	1,205,073,612	5,000,000	137,000,000	11.4 %	11.4 %	62,713,680
Indonesia	248,645,008	2,000,000	55,000,000	22.1 %	5.1 %	51,096,860
Japan	127,368,088	47,080,000	101,228,736	79.5 %	9.4 %	17,196,080
Kazakhstan	17,522,010	70,000	7,884,905	45.0 %	0.7 %	700,020
Korea, North	24,589,122	--	--	--	--	n/a
Korea, South	48,860,500	19,040,000	40,329,660	82.5 %	3.7 %	10,012,400
Kyrgystan	5,496,737	51,600	2,194,400	39.9 %	0.2 %	109,060
Laos	6,586,266	6,000	592,764	9.0 %	0.1 %	255,880
Macao *	578,025	60,000	366,510	63.4 %	0.0 %	210,040
Malaysia	29,179,952	3,700,000	17,723,000	60.7 %	1.6 %	13,589,520
Maldives	394,451	6,000	134,860	34.2 %	0.0 %	136,760

Note: Adopted from *Internet Usage in Asia.* Retrieved February 10, from http://www.internetworldstats.com/stats3.htm

COBIT Security (2004) recognised that with the widespread use of Internet, electronic handheld devices and wireless technologies introduce more threats to the protection of information. Threats such as phishing, data theft, fraud, fire, viruses, denial-of-service attacks and even social engineering pose serious risks to the protection of information (ISO17799, 2005; Pfleeger, 1997).

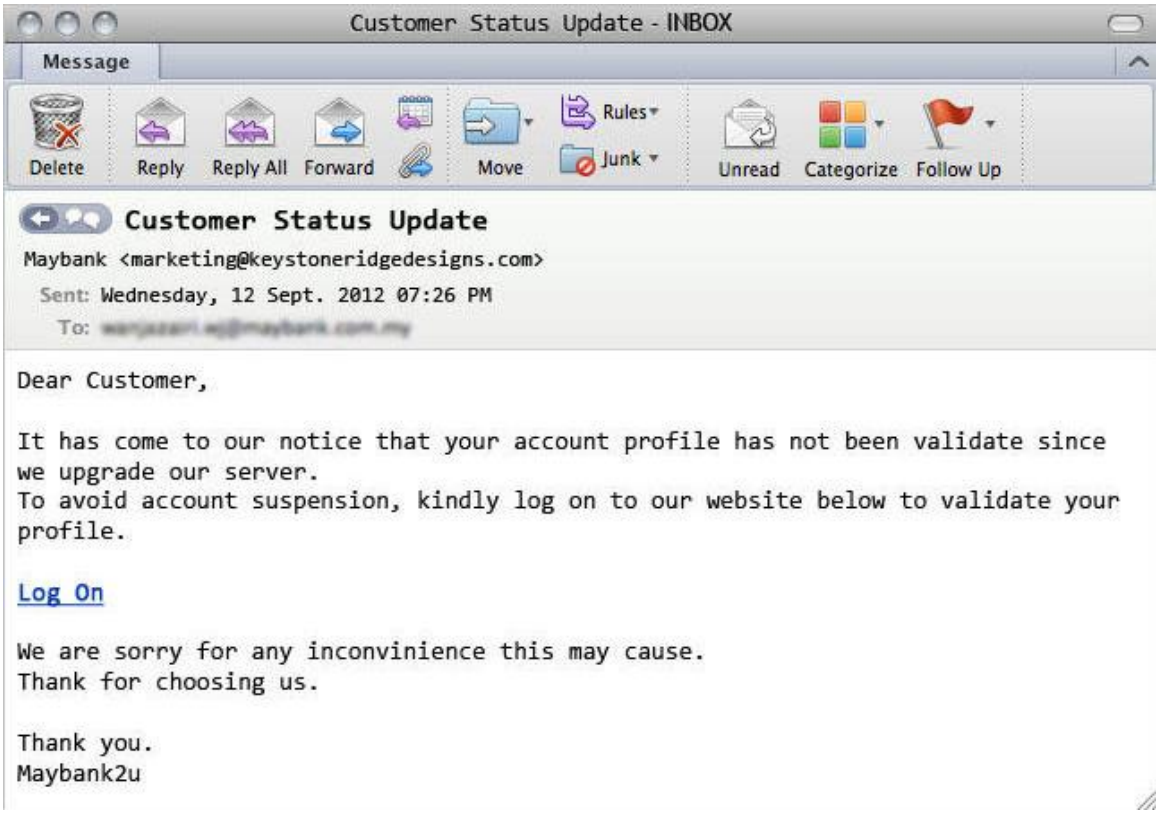
Thus, information security is concerned with implementing adequate controls to protect information assets. However, this controls must aligned with the organisation's security objectives and should minimize the risks which organization is exposed.

2.3 Phishing

Phishing is one the threats being tackled nowadays. It is a growing issue in the current global industry and poses ongoing threats which may affect employees in organisation (Ohaya, 2006; Orgill, Romney, Bailey & Orgill, 2004). According to previous studies, there are many variation of phishing attacks namely spear phishing, business service phishing, crisis-phishing, malware danger, smishing, vishing, pharming and man-in-the-middle (Lungu and Tabusca, 2010; Munir, 2007).

Various forms of phishing attack being detected nowadays. The common phishing schemes mostly use spoofed e-mails to lure users to fake websites designed and provide their confidential information (Ohaya, 2006). The tone or contains in the spoofed e-mails normally tend to threaten the victims as to reply and take actions as soon as possible to avoid any further consequence. A sample of phishing e-mail was attached as per Figure 3 below.

Figure 3: Example of phishing e-mail

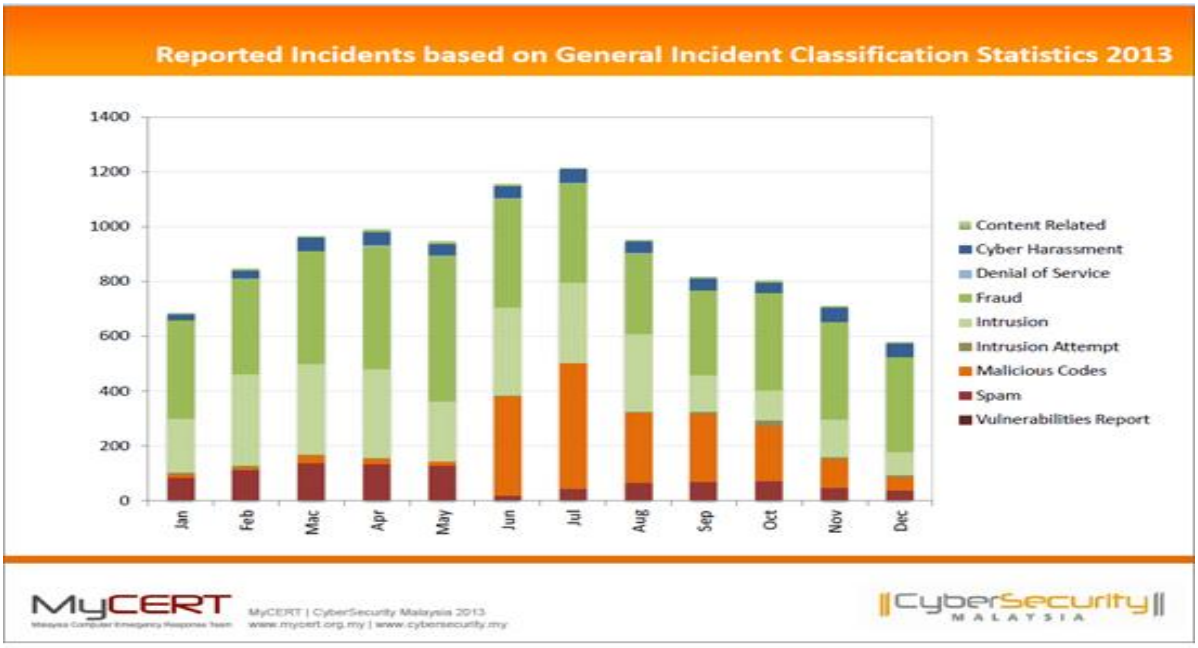


Note: From Google Image. Retrieved November 6, from https://www.google.com/search?q=phishing+e-mail+of+maybank2u&client

Upon updating the personal and financial details, victims are being tricked and resulting in huge financial losses due to the exposure of confidential information (Stair & Reynolds, 2010). Dhamija, Tygar and Hearst (2006) had identified three main factors that contribute to the success of phishing attack which were lack of knowledge about phishing, visual deception and bounded attention.

Without any doubt, the phishing activities also in the trend of increasing with the conjunction of the rise in Internet usage in Malaysia. As reported in MyCert incident statistics 2013 (Figure 4), the fraud cases being reported was 4485, an increase of 12.1% from 4001 cases in 2012.

Figure 4: MyCert incident statistics for year 2013



	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	TOTAL
Content Related	4	7	5	10	8	8	1	1	1	4	2	3	54
Cyber Harassment	21	30	49	48	42	43	49	42	43	40	54	51	512
Denial of Service	0	1	1	4	2	2	2	4	2	0	0	1	19
Fraud	358	346	412	448	530	396	362	292	308	355	334	344	4485
Intrusion	197	336	329	325	218	321	293	284	134	109	139	85	2770
Intrusion Attempt	8	4	4	2	2	4	1	3	11	21	7	9	76
Malicious Codes	12	11	26	17	15	361	459	257	245	199	103	46	1751
Spam	83	111	137	137	129	17	43	66	70	70	49	38	950
Vulnerabilities Report	2	2	3	0	0	4	2	0	0	4	0	2	19
/157/index.html	685	848	966	991	946	1156	1212	949	814	802	688	579	10636

Note: Adopted from *MyCert Incidents Statistics*. Retrieved May 2, from http://www.mycert.org.my/en/services/statistic/mycert/2013/main/details/914/index.html

Malaysia government in their initiative to combat those phishing threats and abuses had formulated and introduced relevant legal frameworks such as Cyber Laws of Malaysia (Mohamed & Masket, 2007). In recent, announcement had been made to all residents in Malaysia with the enforcement of Personal Data Protection Act 2010 which coming into effect on 15th November 2013. This Act will be further discussed in later chapters.

However, the negative impact of phishing can be minimised with proper education and awareness of phishing among consumers (Goh, Tan, Goh & Eze, 2008). In other research, it was found that consumers who have less susceptible to phishing were having better understanding of the internet and how the Internet works, for example, they know how to read the URLs (Downs, Holbrook, & Cranor, 2007).

2.4 Information Security Governance

Over the last two decades, a great deal of research had been done on various aspects of information security, including methods of technically securing a network and the information in that network, developing secure computer systems modeling and mathematical models, developing and utilising information technology and security frameworks, gaining management's support of information security, aligning information technology and security to organisational plans and goals, developing and adhering to information technology and security regulatory requirements, requiring the use of information security awareness training (Kehoe, Little, & Lyons, 1993; Knapp, Marshall, Rainer & Ford., 2006; Li & Chandra, 2007; Smith, Koohang, & Behling, 2010; Stacey & Helsley, 1996; Trim, 2005; Von Solms, 1997; Whitmore, 2001).

Information security has becomes an integral part of daily life. Organisations need to ensure that they are adequately secured (Saint-Germain, 2005). There are a number of best practice frameworks that were designed to help organisations appraise their security risks, establish suitable security controls, follow governance requirements, and handle privacy and information security regulations.

In the context of Malaysia, The National IT Agenda (NITA) was formulated in 1996 to provide the framework for the orderly development of the country into an information and knowledge-based society by 2020. The necessary infrastructure and environment for the development of information and communications technology was in place during the Seventh Plan period to enable Malaysia to move rapidly into the Information Age. Coherence with this plan, Personal Data Protection Act 2010 was just in force by government last year.

Next, several information security governance were briefly discussed in the following sub-chapters which are COBIT, ITIL, ISO 17799 and Personal Data Protection Act 2010.

2.4.1 COBIT

COBIT is the short form of "Control Objectives for Information and Related Technology" which published by IT Governance Institute. COBIT is a high-level governance and control framework that is based on an IT process model that is generically framed to suit any organisation. The framework is intended for users, auditors, management, and business process owners.

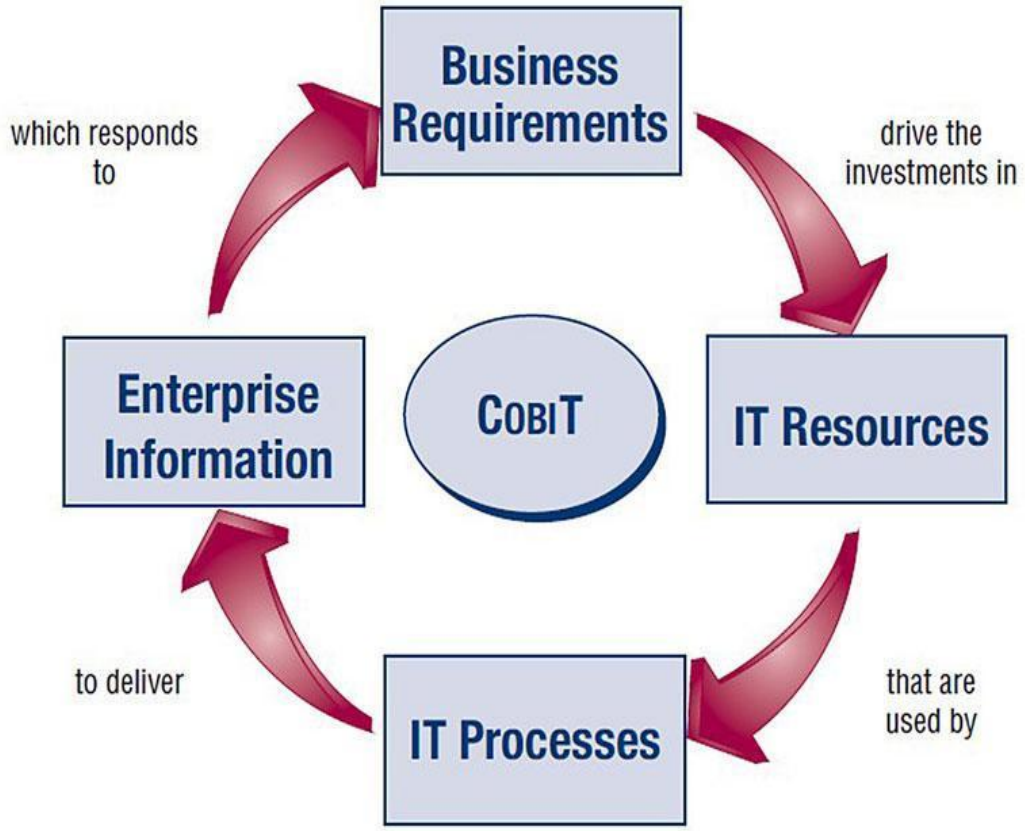
COBIT gives the management of agencies and private-sector organisations the tools necessary to maintain a proper level of control over IT systems while at the same time considering the cost effectiveness of the implementation and maintenance of those controls (Hawkins, Alhajjaj, & Kelley, 2003). COBIT enables management to determine an organisation's most vulnerable areas and to define a level of control that will help ensure the agency has limited loss of valuable information, thereby ensuring the continuity of the services provided.

COBIT also provides the necessary tools to develop a plan of action that ensures a minimal loss of information in the event of a devastating incident. The main point of COBIT is business orientation. COBIT is designed not only to be used by auditors and users, but also by the owners of business-processes. Business practices increasingly require the full authority of business-process owners as they have full accountability for all facets of their business process.

COBIT is obtaining worldwide acceptance as the definitive authority for IT Governance, Control Objectives, and Audit. Additionally, this process is being used by various internal business groups, such as Boards of Directors, CEOs, CIOs, Audit Committees, governmental leadership, Security Managers, and Information Systems Auditors.

Lainhart (2000) suggested that COBIT undertakes the requirement of information and related IT to be properly managed and controlled. Lainhart's article looked at COBIT and how various management levels were using it. The following Figure 5 refers to the framework of COBIT.

Figure 5: COBIT



Note: From COBIT (Control Objectives for Information and related Technology). 2004. *COBIT Security Baseline – An Information Security Survival Kit.* USA: IT Governance Institute.

COBIT provides process framework for information system governance and allows organisations to develop a control structure as to link its IT objectives with business requirements. COBIT breaks down the control structure into four major domains and 34 sub-domains. The major four domains are:

1. Planning and organization (10 processes)
2. Acquisition and implementation (7 processes)
3. Delivery and support (13 processes)
4. Monitoring (4 processes)

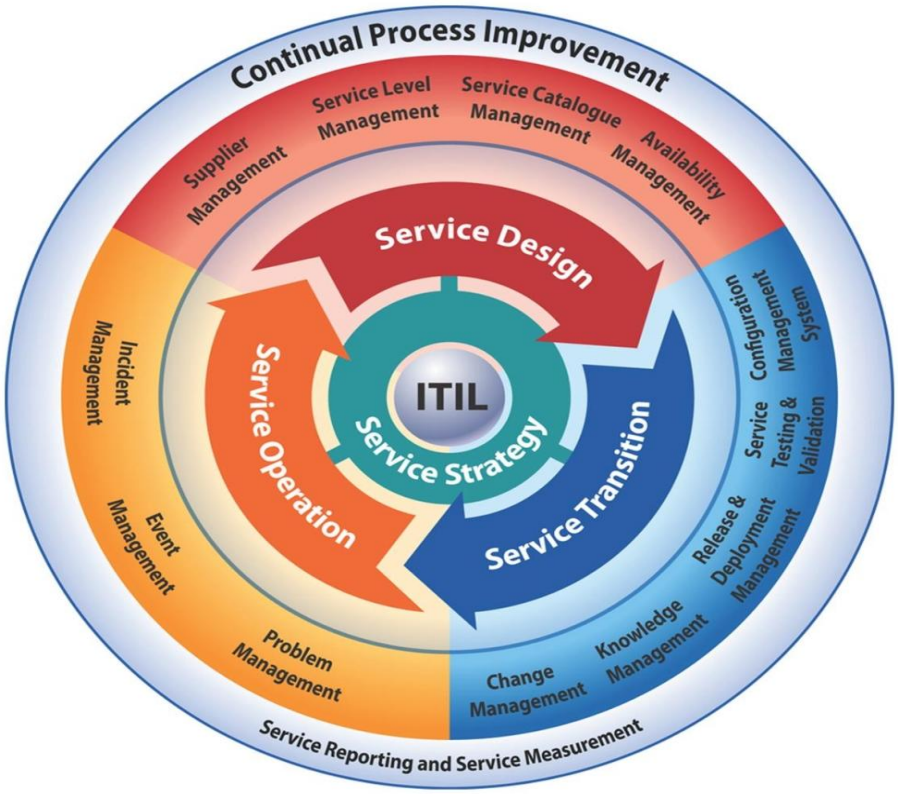
Exclusively, COBIT provides maturity models for control over information technology processes. Thus, management can better define the current position of organisation, level of achievements compare to the best in industry or international standards and to what extent the organisation tend to achieve.

2.4.2 ITIL

ITIL (Information Technology Infrastructure Library) is a collection of procedures and best practices for IT services management and operations. It was developed in the late 1980s by the British government and was popular in Europe throughout the 1990s. The government of the United Kingdom developed and publishes ITIL in order to afford best practices for IT service management.

This document's services are appropriate to the business needs of the organization and are broken down into Service Support and Service Delivery. The service support processes are incident management, problem management, configuration management, change management, release management, and service desk function. The service delivery processes include capacity management, availability management, financial management for IT services, service level management, and IT service continuity management as shown in Figure 6.

Figure 6: ITIL



Anthes (2005) stated that presenting a better face to users is at the best of the ITIL. The Anthes work was a practitioner article that looked at the implementation of this publication and the roles that management plays. Forrester Research Inc. conducted a survey in 2004 indicating that twelve percent of billion dollar companies had adopted some portion of ITIL; while one-third said they were getting started on ITIL or were considering using it.

ITIL has become more popular in the United States recently. Although other alternatives are available, ITIL is still becoming the tools of choice for standardising, integrating, and managing IT service delivery for organisations.

2.4.3 ISO 17799

ISO 17799 is a code of practice which lists a substantial number of specific security controls that may be applicable to an information technology environment. ISO17799 was developed from British Standards Institution publications with the original standard that was issued in two parts:

1. 7799 Part 1 – Information Technology-Code of Practice for Information Security Management.
2. BS 7799 Part 2 – Information Security Management Systems-Specification with Guidance for Use.

ISO 17799 consists of 12 components (Da Veiga, 2008):

1. Security policy – to provide direction to management and support for information security which include laws and regulations.
2. Organisation of information security – comprise of the information security management process being implemented within organization.
3. Asset management – focus on asset inventories, information classification and labeling management.
4. Human resources security – includes awareness, training and education of employees and considers the responsibilities of trading partners, permanent and third party users in order to minimise the misuse of facilities and risk of threats or fraud.
5. Physical and environment security control – facilities and secure areas are strictly access by those authorised people only.
6. Communications and operations management – ensure the information processing facilities operation (e.g. segregation of duties, change

management, malicious code and network security) in correct and secure manners.

7. Access components – manage user access to information and include clear desk principles, network access controls, operating system access controls, passwords and tele-working.
8. Information acquisition, development and maintenance – ensure the user-developed and off-shelf-products are being secured.
9. Information security incident management – ensures that incidents are communicated in a timely manner and corrective action is taken.
10. Business continuity management – business continuity plans being focused and tested.
11. Compliance – comply to those statutory, regulatory or contractual requirements or obligations, law, audit and organisational policy.
12. Risk assessment and treatment – identify, quantify, priorities and treat risks posed to information assets.

Generally, the leading principles of ISO 17799 are for actualising information security. These principles depend on both generally accepted best practices and legal requirements. Besides, ISO 17799 is divide into 10 sections, with 36 objectives.

According to Von Solms (2005), the advantage of using ISO 17799 is that ISO 17799 provides much more guidance on specifically the ways to carried out and it is also more detailed than COBIT. However, due to the narrow focus, it makes ISO 17799 turns to be stand alone guidance which not integrated into wider framework for information technology governance.

Figure 7: ISO 17799

Note: From ISO. 2005. Information Technology Security Techniques. Code of Practice for Information Security Management. ISO/IEC 17799 (BS 7799-1: 2005).

2.4.4 Personal Data Protection Act 2010

Personal Data Protection Act 2010 was in force and effective on 15th November 2013. As stated in the Act, the penalty for non-compliance will be between RM100,000.00 to the maximum of RM500,000.00 and/or imprisonment of between 1 to 3 years. The Act introduces a comprehensive personal data protection regime that imposes broad obligations on those who process personal data in connection with commercial transactions.

Personal data was defined under the Act as "any information in respect of commercial transactions, which –

(a) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;

(b) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or

(c) is recorded as part of a relevant filing system or with the intention that it should form part of relevant filing system,

that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject; but does not include any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010."

Further, as summarised in the article written by Foong and Bakar (2013), this Act is only apply to:

1. personal data which is processed;

2. any person who processes and any person who has control over or authorises the processing of any personal data in respect of commercial transactions and such a person is a "data user"; and

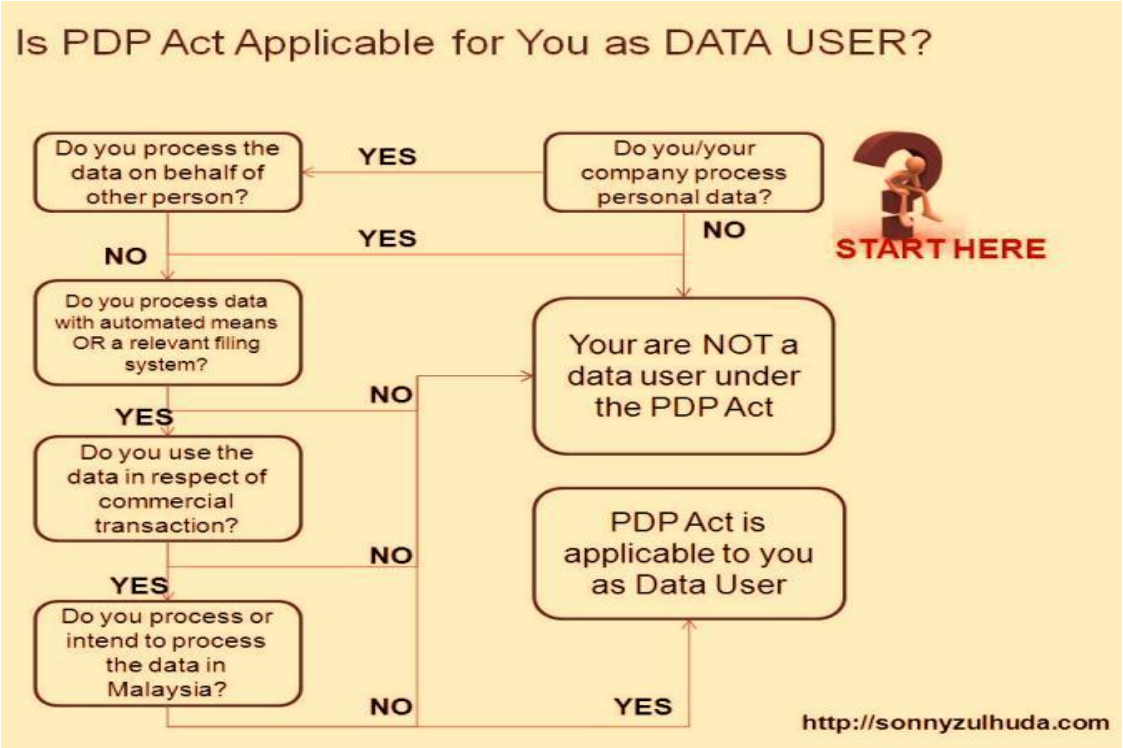
3. to a person in respect of personal data if-

   (a) the person is established in Malaysia and the personal data is processed, whether or not in the context of that establishment, by that person or any other person employed or engaged by that establishment; or

(b) the person is not established in Malaysia, but uses equipment in Malaysia for processing the personal data otherwise than for the purposes of transit through Malaysia.

With the enforcement of this Act, personal data life cycle management process is affected as from the beginning point of the data being collected, used, stored and disposed. In such, business operations will definitely affected as the process of handling data will need to be redefined in order to comply with the Personal Data Protection Act 2010. According to Zulhuda (2012), a central repository may be required for consent management. Consequently, the complexity of process being increased when deal with the cross border personal data transfer. Further, Zulhuda (2012) provide a diagram (Figure 8) for self-checking on who is needed to comply with the Act.

Figure 8: Personal Data Protection Act 2010



Note: From Zulhuda, S. (2012). Personal Data Protection Act 2010 will be enforced from 01.01.2013-or so it was said…. Retrieved December 12, from http://sonnyzulhuda.com/2012/10/23/personal-data-protection-act-2010-will-be-enforced-from-01-01-2013/

2.5 Information Security Governance Compliance

Information in the modern electronic world can be viewed as the most important asset in global market. Individuals, organisation and government depend on information to be secured and private by trustworthy information technology.

Most companies are trying their best to combat information security threats and risks within their organisations. A majority of these companies implement information security through technical and operational controls but don't understand or know how to focus their efforts and resources on the different areas and techniques that will produce the desired information security results (Ezingeard & Birchall, 2007; McFadzean, Van Niekerk & Von Solms, 2010).

As quoted by IBM Business Consulting Services (2006), individuals within an organisational environment often tend to rely on an organisation to take responsibility and have these well defined controls to protect the integrity and availability of their personal data from unauthorised access, use, disclosure, disruption, modification or destruction.

In other way, employees may ignorantly or negligently contribute to information security risks. For example, by unwittingly retrieving spam electronic mail, opening virus e-mail attachments, or dismissing information security threats as unimportant in comparison with other needs such as usability (Besnard & Arief 2004).

In previous survey (McAfee 2005), findings of insider misuse included:

1. 21% of workers allowed family and friends to use company laptops and personal computers for internet access.

2. 51% of workers connect their own devices or gadgets to their company personal computer.
3. 60% of workers stored personal content on their company personal computer.
4. 10% of workers download prohibited content at work.

Compliance relates to ensuring that the organisation complies with international and national laws as well as industry regulations pertaining to the protection of information (Sherwood, Clark & Lynas, 2005). It is important to measure and take compliance in force according to Von Solms (2005). Management should monitor both technology and employee behavior to ensure its compliances toward information security governance (Vroom & Von Solms, 2004).

2.6 Education and Training

It was stated in ISO/IEC 17799 (2005) that "all employees of the organisation and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organisational policies, procedures, as relevant for their job function". Users must therefore receive training, which could include induction training presentations, Web-based training or group discussion.

According to Herold (2010), education and training are important due to the reasons of regulatory requirements compliance, to gain and keep customers' trust and satisfaction, compliance with published policies, due diligence, corporate reputation and accountability. Thus, providing the employees with the security

and privacy information they need and ensuring they understand and follow the requirements is an important component of organisation's business success.

2.7 Trust

Trust is important when implementing information security. It aids in providing confidence to information users when making decisions. Flowerday and Von Solms (2006) remark that "confidence in information security management requires trust and trust requires information security to help safeguard it".

Martins and Van Der Ohe (2003) defines trust as "the process in which a trustor relies on a trustee (a person or group of people) to act according to specific expectations that are important to the trustor without taking advantage of the trustor's vulnerability".

Trust must be occurs in between management and employees when implementing the information security components. Management should trust in employees to adhere to information security governance while employees should trust in management to illustrate commitment to information security (Robbins, 2001).

Beside management and employees, trading partners and clients who relate to organisation's reputation should be attached with the trust in between. In order to establish the trust in between those trading partners and clients, organisation could show to them how will be those information assets are secured and that employees are comply with information security governance.

2.8 Employee Awareness

Awareness can be explained as the different activities that the organisation deploys to reinforce information security requirements and responsibilities required by the information security policy (SOGP 2003). Mcllwraith (2006) believes that awareness is the "single most effective thing an information security practitioner can do to make a positive difference to their organisation".

According to Furnell, Gennatou & Dowland (2002), the need to promote information systems security standards within organisation requires information systems security awareness training. Furnell also proposes that all users should be aware of disciplinary actions resulting from non-compliance with organisation's information systems security procedures.

Similarly, Denning (1999) argues that information systems awareness training and education is an essential part of defending information systems security. The awareness program should communicate to users the organisation's information systems security governance and make users aware of the risks and potential losses cause by the non-compliance. It was suggested that e-mail communication or posters can for instance be used to raise awareness about information security requirements.

2.9 Ethical Conduct

Ethics were defined as the values and rules that differentiate the right from wrong by Hellriegel, Slocum and Woodman (1998). Example, employees should not discuss about confidential information in public places. According to Hartmann (1995), ethics in information technology is such a large question that systems designers, developers and users are not alone enough to give answers. Instead, entire society should be involved in the discussion concerning responsibilities of different groups involved.

Kowalski (1990) has identified four major reasons for ethical issues to appear in the computer security research. First of all, there is the widening control gap in commercial information systems whereby the control gap can be further divided into three categories which refer to technological gap, social-technical gap and social gap. Second, ethics may be the common language for specialists of different areas and can be understood also by groups outside the computing community.

Third, current systems are so large that there are no implicit technological control structures to manage them. Lastly, there is the need for top-down approach as in the Information Systems Secure Interconnection (ISSI) model. Five non-technical layers are added on top of OSI protocols and the ethical is at the uppermost layer.

2.10 Privacy

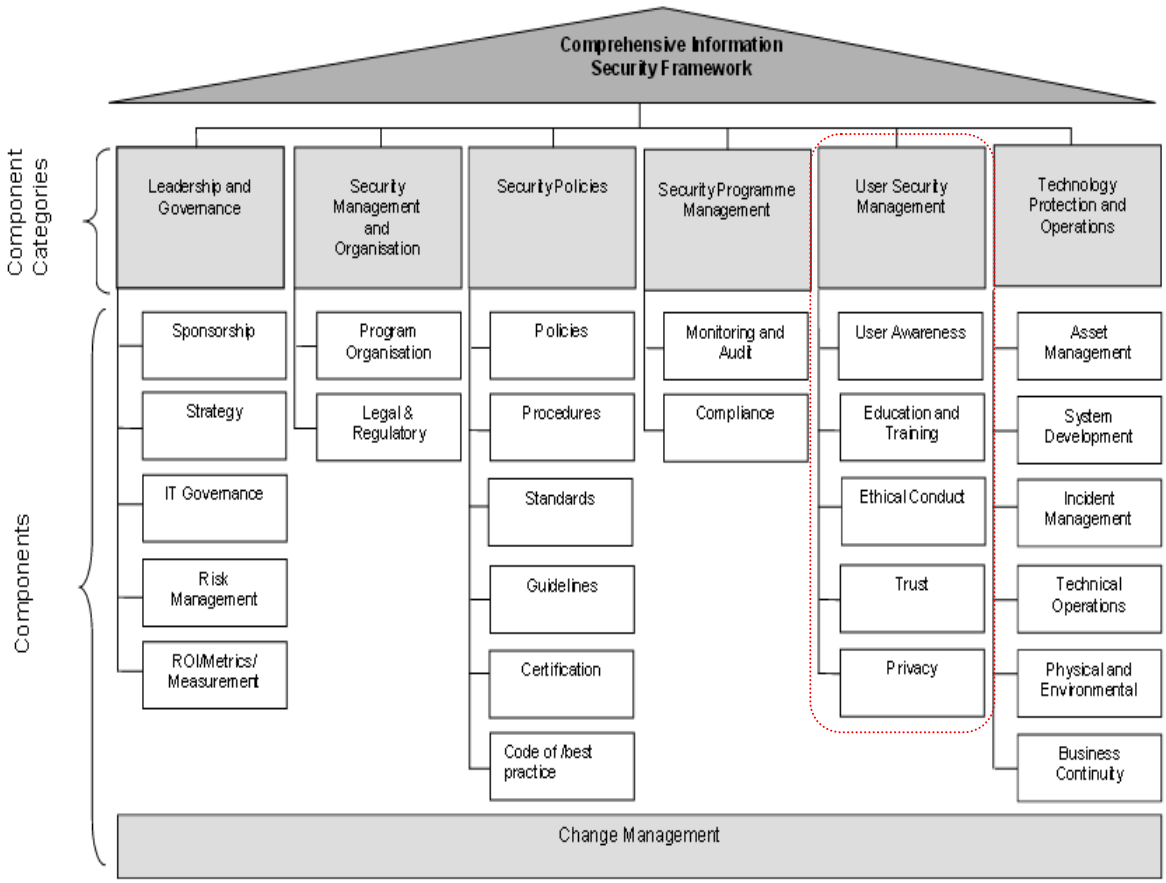
Stated by Borking (2006) and Sartor (2008), privacy is another important issue of trust and trust will not exist if there is no privacy. Controls must be implemented and both employees and clients must also be considered during information secure privacy implantation in order to protect the personal identifiable information of individual (ISACA, 2005; SOGP, 2003).

Personal identifiable information refers to name and surname, identification number, address and etc. it is widely defined as information which directly or indirectly to an individual who is identifiable through out the provided information. Thus, organization had to ensure that those personal information of employees, trading partners, clients or even third parties which hold in the organization being control properly.

2.11 Theoretical Framework

Figure 9 shows the developed theoretical framework for this study. The theoretical framework was partially adopted as highlighted from Da Veiga (2008) study on cultivating and assessing information security culture. Da Veiga (2008) developed a Comprehensive Information Security Framework (CISF) which equips organisations with a holistic approach to the implementation of information security.

Figure 9: Comprehensive Information Security Framework (CISF)



Note: From Da Veiga, A. (2008). Cultivating and assessing information security culture. *Information Systems Mangement*. 24(2), 361-372.

According to Da Veiga (2008), the user security management category comprised user awareness, education and training, ethical conduct, trust and privacy as the component for that category. All the components stated are related to employees and the ways of directing employee's behavior in organisation.

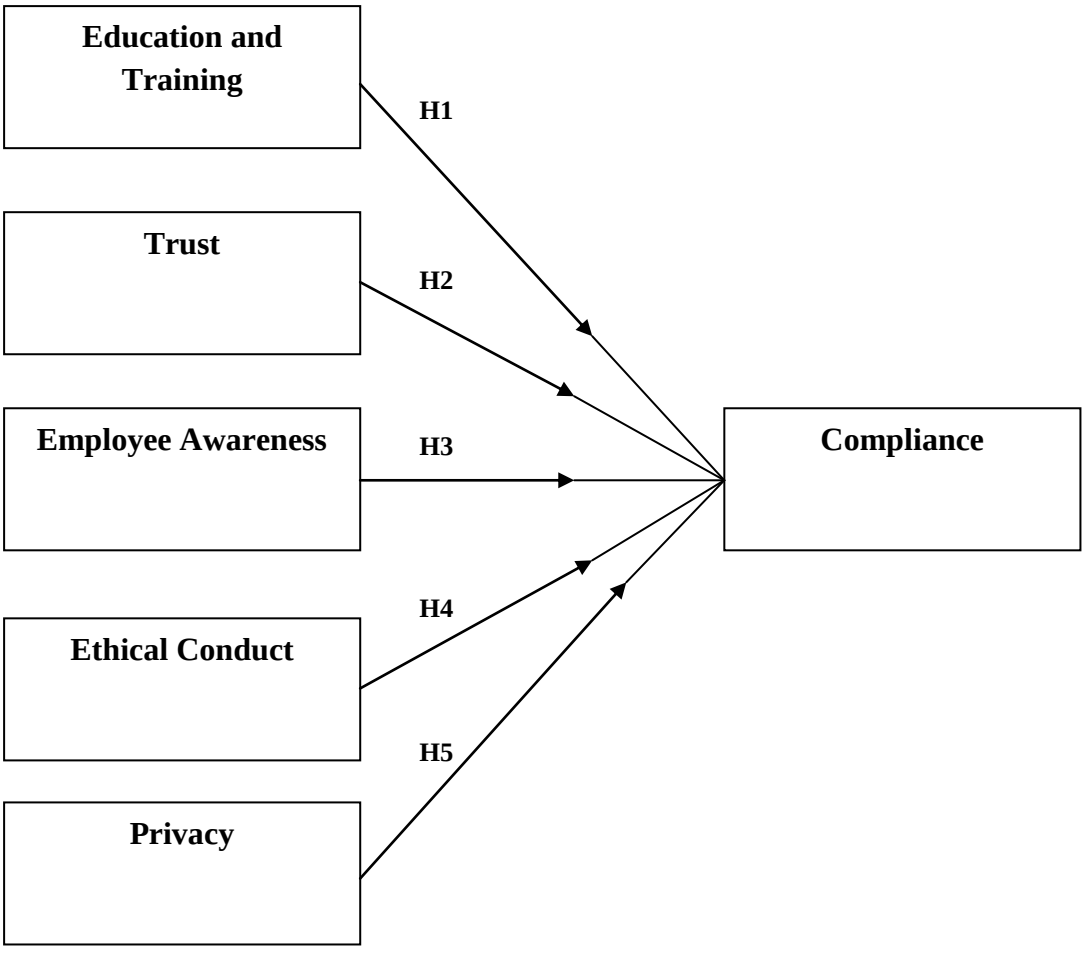
Other researcher which focus on employees toward information security governance compliance like Colwill (2009), the study found that insiders are on of the threats for organization information security. Further, a single-case study in Taiwan by Ku, Chang and David (2009) which also focus on employees conclude that factors which affect self-implementation by employees were past experience, degree of understanding, support from top management and education and training.

Besides, a number of research categories from an information security perspective are relevant when focusing on the human element in information security. For example, information security policy obedience (Siponen, Pahnila & Mahmood, 2007; Vroom & Von Solms, 2004), information security awareness (Kruger & Kearney, 2006; Puhakainen, 2006) and inside computer crime (Cardinali, 1995). All are aiming at minimising the threat that user behavior poses to the protection of information assets.

2.12 Conceptual Framework

The conceptual framework derived by researcher in this study will be shown in Figure 10 as follow. In this study, the relationship between education and training, trust, employee awareness, ethical conduct and privacy toward compliance on information security governance were examined.

Figure 10: Conceptual framework



2.13 Hypothesis

As quoted by Swanson and Holton (2005), “a hypothesis is a proposition that there is a relationship between variables”. The significant level is set at 0.05 whereby the P-value should less than 0.05 in order to conclude that the tested variables have significant relationship.

The following hypotheses were tested to answer the research questions:-

(a) Hypothesis 1:

Education and training has significant relationship toward compliance on information security governance.

(b) Hypothesis 2:

Trust has significant relationship toward compliance on information security governance.

(c) Hypothesis 3:

Employee awareness has significant relationship toward compliance on information security governance.

(d) Hypothesis 4:

Ethical conduct has significant relationship toward compliance on information security governance.

(e) Hypothesis 5:

Privacy has significant relationship toward compliance on information security governance.

2.14 Summary

The rise of Internet usage and advancement of today's technologies had lead to the rise of phishing issue. It is because the convenience and easy access of Internet usage being explore to the hackers too. Several information security governance as like COBIT, ITIL and ISO 17799 which are consider worldwide used had been introduced since the security incidents issue raised. Malaysia's government also working hard to minimise the fraud cases with the enforcement of CyberLaws of Malaysia and recently Personal Data Protection Act 2010.

Management always being reminded that such information security governance should developed accordance and align to their business goals, missions and operations. Beside employee's awareness, other factors like education and training, trust, ethical conduct and privacy might also influence the compliances of information security governance. In order to having a sustainable information security governance, implementation and review should carried always.

Five hypotheses had been drawn and the framework for this study was adopted from Da Veige (2008)'s thesis, whereby researcher wish to examine the relationship of five key factors with compliance on information security governance.

CHAPTER 3

METHODOLOGY

3.1 Overview

Chapter 3 discusses the overall progress and the methodologies of this study being conducted and adopted by the researcher. Research design (sub-chapter 3.2.1) refers to the selection and determination of type of research and method for this study according to Saunders, Lewis and Thornhill (2012) research 'onion'.

Questionnaire development was being expressed in the following sub-chapter of 3.2.2. A cover letter was attached to the questionnaire and it was being sectioned into four. The sources or input for each of the questionnaire statements had been tabulated. Reliability and validity of data (sub-chapter 3.2.3) collected was tested against Cronbach's coefficient alpha value.

Variables measurement (sub-chapter 3.2.4) was conducted using five point Likert scale from *strongly disagree* to *strongly agree*. Additionally, the summary of questions to variables also had been tabulated.

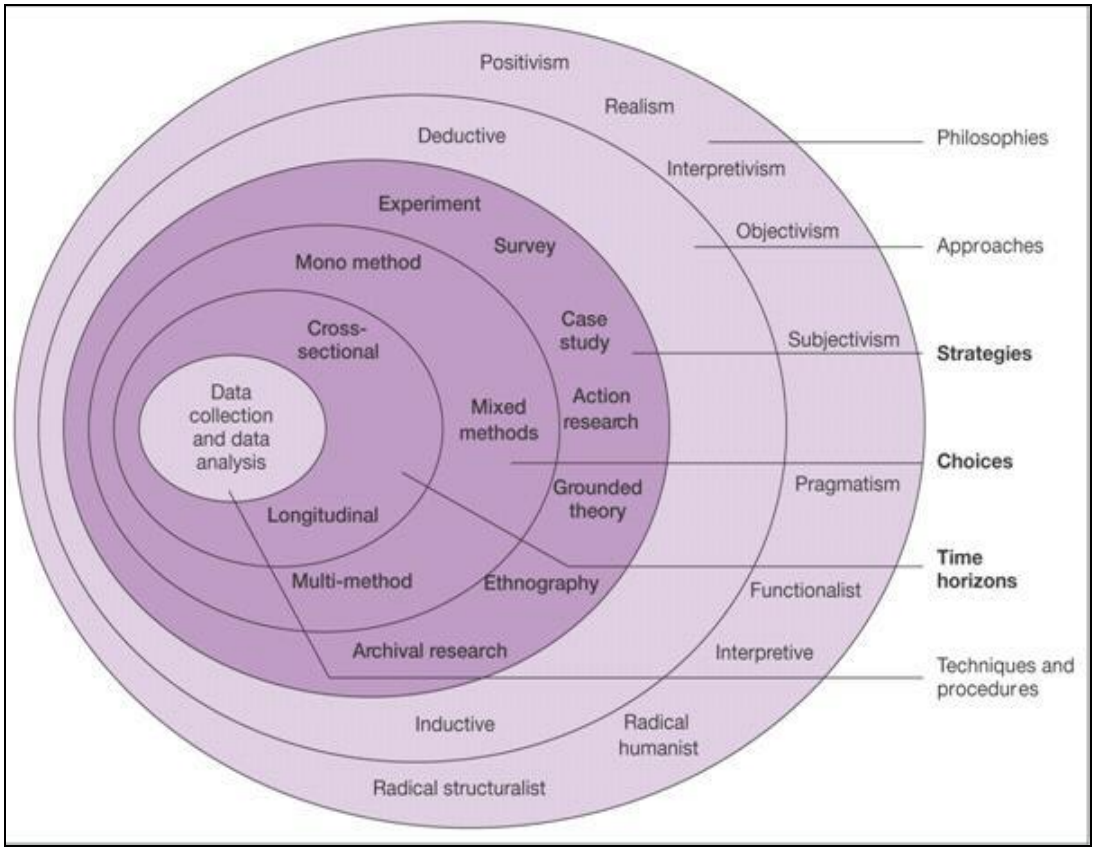
Population (sub-chapter 3.4.1) was stated and sampling (sub-chapter 3.4.2) method was explained to judge the logical behind on the selected sampling method being used. Data collection (sub-chapter 3.4.3) was conducted through an online survey instrument media and the selected channel for questionnaire distribution was stated. A table inserted to present the data coding (sub-chapter 3.4.4) in this study.

Data analysis (sub-chapter 3.4.4) refers to the tools and statistical approaches being used to analyse the collected data. Lastly, what ethical issues that had taken into consideration (sub-chapter 3.5) and summary (sub-chapter 3.6) of this chapter being written as.

3.2 Research Design

The research design in this study is being drawn according to the Saunders et. al., (2012) research 'onion' as attached in Figure 11.

Figure 11: The research 'onion'



Note: From Saunders, M., Lewis, P., & Thornhill, A. (2012). *Research methods for business students* (6th ed.), UK: Pearson Education Limited.

Mono quantitative research method had been selected by the researcher in term of methodological choice. As the characteristics of mono quantitative research design enable researchers to examine the relationship between variables, which are analyzed using a range of statistical techniques and measured numerically (Saunders et al., 2012).

Beside, only single data collection technique (survey) being adopted in this study as the choice of mono qualitative research method. In order to accept or reject the hypotheses drawn, the nature of this research is being recognized as explanatory studies. As the hypotheses in this study were tested against the significant relationship among the five independent variables and dependent variable.

According to Phellas, Block and Seale (2011), bias of response which caused by the interviewer and interviewee can be reduced by using the questionnaire method. As such, researcher in this study had developed a questionnaire and it will be used as the survey instrument. In other word, survey being adopted as the strategy of this study. Yet, it is one of the common and popular strategy being adopted in most of the business and management research (Saunders et al., 2012).

Due to time constraint, this survey strategy study is a cross-sectional study. Practically, most of the academic research projects are undergo as a cross-sectional study. It is due to necessarily time constrained in all the academic courses.

3.2.2 Development of Questionnaire

In order to assess employees' knowledge and perceptions on the six variables, questionnaire validated in previous research were combined to create the survey instrument for this study. Some of the wordings were being modified to suit the study context.

The following tables show the statements of this study's survey instrument with the first column states the questionnaire statements under each of the tested

variables and knowledge statements. In the second column, theoretical references used in the survey instrument were listed as the sources of questionnaires development. In the third column, a cross mark (**X**) indicates that such statement is an input from the industry as opposed to theory.

A cover letter was attached at in this study's survey instrument. Objectives, significant of this study, time to be taken for the completion of survey, confidentiality of participants and researcher's contact were being explained and included in the cover letter. It is to ensure that participants could feel more comfortable while answering the questions.

There are four sections in the survey instrument:

- Section 1: Demographic
    - General demographic data of participants which are gender, age group, education level, ethnicity, type of business/industry and year(s) in organisation.
- Section 2: Knowledge statement
    - Total of 11 questions in Section 2 being generated.
- Section 3: Variables measurement statement
    - Independent variables: Education and training, Trust, Employee awareness, Ethical conduct and Privacy.
    - Dependent variable: Compliance.
    - Total of 31 questions in Section 3.
- Section 4: Conclusion statement
    - To assess the perception of participants' about information security policy after completing this survey instrument.
    - Total of 6 questions being asked.

Table 1: Questionnaire statements' sources

Questionnaire Statements		Theoretical References	Industry Input
Knowledge Statements			
1	I believe that my current working company has a written information security policy.	ISO/IEC 17799:2005	
2	I have read the information security policy sections that are applicable to my job.		X
3	I understand the information security policy.		X
4	I know what information security is.	ISO/IEC 17799:2005	
5	I know where to get a copy of the information security policy.		X
6	I know what my responsibilities are regarding information security.		X
7	I am informed of information security requirements to protect information.	ISO/IEC 17799:2005; Mcllwrath (2006); SOGP (2003)	
8	I know what the risk is when opening e-mails from unknown senders, especially if there is an attachment.		X
9	I know how to use the anti-virus software to scan for viruses (e.g. when I download files from the internet).	ISO/IEC 17799:2005	
10	When I leave my computer, I always lock the screen.	ISO/IEC 17799:2005	
11	At the end of the day, I ensure that there are no confidential documents left in my working area.	ISO/IEC 17799:2005	
Education and Training			
1	The contents of the information security policy were effectively explained to me.	Dojkovski, Lichtenstein, Warren (2006)	
2	I believe there is a need for additional training to use information security controls in order to protect information.		X
3	I believe the information security awareness initiatives are effective.	Dojkovski, Lichtenstein, Warren (2006); ISO/IEC 17799:2005	
4	I received adequate training to use the applications I require for my daily duties.	Dojkovski, Lichtenstein, Warren (2006); ISO/IEC 17799:2005	

Table 1: Questionnaire statements' sources (continued)

	Questionnaire Statements	Theoretical Reference	Industry Input
5	The information security policy, procedures and guidelines clearly state what is expected of me to safeguard information.	Von Solms & Von Solms (2003); Gaunt (2000)	
Trust			
6	I believe that management communicates relevant information security requirements (e.g. what Internet usage is allowed, how to make backups, security usage of removable media such as USB's/PDA's) to me.		X
7	I believe that Information Technology (IT) business unit implements information security controls (e.g. restricting access to secure areas, controlling access to computer systems, preventing viruses).		X
8	I believe that IT business unit has adequate authority to ensure the implementation of information security governance.	McCarthy & Campbell (2001)	
9	I believe that organization pays adequate attention to an information security strategy in order to protect information.	CISA 2005; Sherwood, Clark & Lynas (2005)	
10	I believe the IT business unit adequately assists in the implementation of controls to protect information.	McCarthy & Campbell (2001)	
Employee Awareness			
11	Information security is necessary in my business unit to protect information.	Mcllwraith (2006)	
12	The employees in our business unit perceive information security (e.g. sharing confidential information) as important to protect information.	Mcllwraith (2006)	
13	I am aware of information security aspects relating to my job (e.g. when to change my password or which information I work with is confidential).	Mcllwraith (2006)	
14	It is necessary to protect information to achieve the business strategy of organization.	CISA 2005; Sherwood, Clark & Lynas (2005)	
15	There are adequate information security specialists/coordinators throughout my organization to ensure the implementation of information security controls.		X

Table 1: Questionnaire statements (continued)

	Questionnaire Statements	Theoretical Reference	Industry Input
Employee Awareness			
16	The information security controls implemented by organization support the business strategy.	CISA 2005; Sherwood, Clark & Lynas (2005)	
Ethical Conduct			
17	I accept responsibility towards protection of information.	Cardinali 1995	
18	I think it is important to regard the work I do as part of the intellectual property of company.		X
19	I believe it is important to take care when talking about confidential information in public places.		X
20	I believe that e-mail and Internet access are for business purposes and not personal use.		X
21	I believe my colleagues comply with copy right laws.		X
22	I believe that sharing of passwords should be used to make access to information easier.		X
Privacy			
23	I believe that third parties who have access to confidential information preserve the confidentiality thereof.	ISACA 2005; SOGP 2003	
24	There are clear directives on how to protect sensitive (confidential) clients' information.	ISACA 2005; SOGP 2003	
25	There are clear directives on how to protect sensitive (confidential) employees' information.	ISACA 2005; SOGP 2003	
26	I believe that management keeps my private information (e.g. salary or performance appraisal information) confidential.	ISACA 2005; SOGP 2003	
27	I believe that the information I work with is protected adequately.	ISO/IEC 17799:2005	
Compliance			
28	My business unit enforces adherence to the information security policy.	Von Solms (2005); Vroom & Von Solms (2004)	
29	Employees in our business unit adhere to the information security policy.	Von Solms (2005); Vroom & Von Solms (2004)	

Table 1: Questionnaire statement (continued)

Questionnaire Statements		Theoretical Reference	Industry Input
Compliance			
30	Action should be taken against anyone who does not adhere to the information security policy (e.g. of they share passwords, give out confidential information of visit prohibited Internet sites).		X
31	I should be held accountable for my actions if I do not adhere to the information security policy.	Von Solms (2005); Vroom & Von Solms (2004)	
Conclusion			
1	It has made me more worried about the information security policy.	Furnell, Bryant & Phippen (2007)	
2	It has made me more confident about my own knowledge on information security policy.	Furnell, Bryant & Phippen (2007)	
3	It has increased my awareness of information security policy as an issue.	Furnell, Bryant & Phippen (2007)	
4	It has made me realize I don't understand as much as I thought.	Furnell, Bryant & Phippen (2007)	
5	It has made me realize I don't do as much as I could.	Furnell, Bryant & Phippen (2007)	
6	It is the same as before I taking this survey.	Furnell, Bryant & Phippen (2007)	

3.2.3 Reliable and Validity Analysis of the Instrument

According to Tavakol and Dennick (2011), Lee Cronbach developed the Cronbach's coefficient alpha in year 1951 to test against the consistency reliability among the variables. Cronbach's coefficient alpha estimate will be utilised as a reliability test for all variables in the research instrument.

Cronbach's coefficient alpha is range from 0 to 1.0, the higher of value generated indicate the more reliable of data (Webb, Shavelson & Haertel, 2006). Webb et al. (2006) also suggest that the Cronbach's alpha value should be at least 0.80 as to support the reliability and consistency of data.

According to Sekaran (2003), the Cronbach's alpha value is consider to be good when it is 0.8 or higher, consider to be acceptable when it is 0.7 and considered poor when it is lower than 0.6. However, the Cronbach's alpha values for all dimensions that ranges from 0.60 to 1.0, exceeding the minimum alpha of 0.6 (Hair, Black, Babin, Anderson & Tatham, 2005), would deem the constructs reliable.

3.3 Data Collection

3.3.1 Variable Measurement

Six demographic questions and forty two survey questions were included in the survey instrument as summarised in the following Table 2. The items selected for each construct were mainly adapted from prior research studies. It took approximately 10 minutes or less for the participants to complete the survey instrument as per Appendix A.

Table 2: Survey instrument questions to variables

		Measurement Questions	**Variable Measured**
Section 1	Demographic Questions	Question 1 to 6	Not Applicable
Section 2	Survey Questions	Questions 1 to 11	Knowledge Statement
Section 3	Survey Questions	Questions 1 to 5	Education and Training
		Questions 6 to 10	Trust
		Questions 11 to 16	Employee Awareness
		Questions 17 to 22	Ethical Conduct
		Questions 23 to 27	Privacy
		Questions 28 to 31	Compliance
Section 4	Conclusion	Questions 1 to 6	Not Applicable

3.4 Population, sampling and data collection

3.4.1 Population

Population is defined as the full set of cases from which a sample is taken (Saunders et al., 2012). In this study, the population is refers to the entire group of employees in Malaysia. Meanwhile, the sample being chosen to conduct this study will be those employees who work in Malaysia.

3.4.2 Sampling

In view of the sampling technique, a convenience sampling method is being adopted by the researcher in this study whereas a convenience sampling is grouped under non-probability sampling. Convenience sampling also known as haphazard sampling or availability sampling (Saunders et al., 2012). With adoption of convenience sampling method, researchers able to sort out the problems of time and cost constraint during the research.

Creswell (2003) suggested that sample size should fall within 25 to 30 participants for those general studies. In such, researcher of this study had set the target respondents at the quantity of about 100.

3.4.3 Data Collection

An online survey instrument, *Google Drive* was used in this study to collect those preliminary data from employees who work in Klang Valley. Comparatively, *Google Drive* provides a better channel for researchers to collect data especially for students. It is free and user-friendly and thus, reduces the hassle of uploading and spreading the questionnaire to target respondents.

The link of the questionnaire being posted to the "UTAR Secret Underground Society Facebook" group's page and researcher's Facebook page. On the other hand, the link was copied and sent through Watsapp mobile application in order to achieve the target sample size of 100 respondents.

3.4.4 Data Coding

Demographic data coded as per Table 3.

Table 3: Demographic coding

Demographic	**Code**					
	1	**2**	**3**	**4**	**5**	**6**
Gender	Female	Male				
Age group	< 20	20 – 29 years old	30 – 39 years old	40 - 49 years old	50 years old and above	
Education level	Primary school	Secondary school	Bachelor degree	Postgraduate degree	Other	
Ethnicity	Malay	Chinese	Indian	Other		
Type of business or industry	Financial	Government	Services	Manufactu-ring	Merchandise / Sales	Other
Year(s) in organization	< 1 year	1 – 3 years	4 – 7 years	8 – 10 years	> 10 years	

The knowledge statement, perceptions of participants concerning the five independent variables and dependent variable and conclusion statements in the survey instrument were being measured by five-point Likert scale in the survey which are anchored by *1-Strong Disagree; 2-Disagree; 3-Neutral; 4-Agree; 5-Strongly Agree* (Fowler, 2009; Swanson & Holton, 2005).

3.4.5 Data analysis

Data collected in *Google Document* were exported into the statistical analysis software application - SPSS (Statistical Package for the Social Sciences) for the study and analysis.

Reliability test was run to test on the validity and reliability of all the variables which having total items or statements of 31. Next, descriptive analysis was carried on those demographic questions' data. Consequently, t-test was generated as to examine the differences between genders among the variables. Lastly, Pearson correlation analysis and multiple linear regression being formulated from the data collected.

3.5 Ethical consideration

Ethical considerations were taken into account in regards to all survey participants. Thus, all survey participants were remain anonymous and only general information such as gender, age group, education level, ethnicity, industry category, and number of years worked being recorded in this study.

Beside, all participation in this study is purely voluntary without any coercion by the researcher. All participants had the right to make the withdrawal at any time during the survey. The collected survey data will be kept securely by the researcher for two years in a removable electronic storage device in order to comply with the safeguarding of data.

3.6 Summary

Overall progress and the methodologies of this study had been written in this chapter. The research design was formulated with refers to Sunders et. al. (2012) research 'onion'. Questionnaire were developed with attach to a cover letter as guiding the participants towards the contents of the survey instrument. Total of 4 sections which comprise of 53 questions being structured in the survey instrument.

Data was collected through Google Documents which enable researcher collect, store and export those data into spreadsheet and later transform into SPSS for data analysing. Data was coded in order to simplify the result interpretation. Lastly, ethical consideration was discussed.

CHAPTER 4

RESEARCH RESULTS AND INTERPRETATION

4.1 Overview

In term of preliminary data analysis, coding for variables was done and presented in table form. Missing data and reliability analysis being discussed in the following sub-chapter. Descriptive analysis was generated for six demographic data. Mean score was generated for the data collected for knowledge statements, all variables and conclusion statements.

Beside, comparison within genders against their perception in knowledge statements, all variables and conclusion statement had been tested. Multivariate normality carried to test on the normality of data. Thus, multicolinearity test was run to test against the independent variables. Analysis of variables was being discussed and multiple linear regression model being formulated after the hypothesis test result being interpreted.

4.2 Preliminary Data Analysis

Total of 108 respondents were collected within the given timeframe of one month in this study. All the statements in the survey instrument had been coded as per Table 4 for further data analysis and interpretation in the following sub-chapters.

Table 4: Variables coding

Section	Description	Measurement Questions	Coding
Section 1	Demographic Questions	Questions 1 to 6	Not Applicable
Section 2	**Knowledge statement**	Questions 1 to 11	**K1** to **K11**
Section 3	**Education and training**	Questions 1 to 5	**ET1** to **ET5**
	Trust	Questions 6 to 10	**T1** to **T5**
	Employee Awareness	Questions 11 to 16	**EA1** to **EA6**
	Ethical Conduct	Questions 17 to 22	**EC1** to **EC6**
	Privacy	Questions 23 to 27	**P1** to **P5**
	Compliance	Questions 28 to 31	**C1** to **C4**
Section 4	**Conclusion**	Questions 1 to 6	**CON1** to **CON6**

4.2.1 Missing Data Analysis

No missing data being found in this study. It was due to the researcher had pre-set each of every questions as the “required question” in the online survey instrument. With such setting, all participants have to complete the question which first attempted to them in order for them to continue and proceed to other questions and submit once all questions had been answered.

4.2.2 Reliability Analysis

The Cronbach's alpha value shown in Table 5 is 0.941 as tested against thirty one questions. The reliability of this survey instrument had been achieved as the Cronbach's alpha value is above minimum value of 0.60.

Table 5: Reliability Analysis

Reliability Statistics

Cronbach's Alpha	Number of Items
0.941	31

4.3 Descriptive Analysis

Frequency analysis was used to analyze those demographic data as mean score is meaningless in those coded data. In the following sub-chapters, demographics statistic were presented in both bar-chart and table form.

4.3.1 Demographic Statistics

Figure 12: Gender

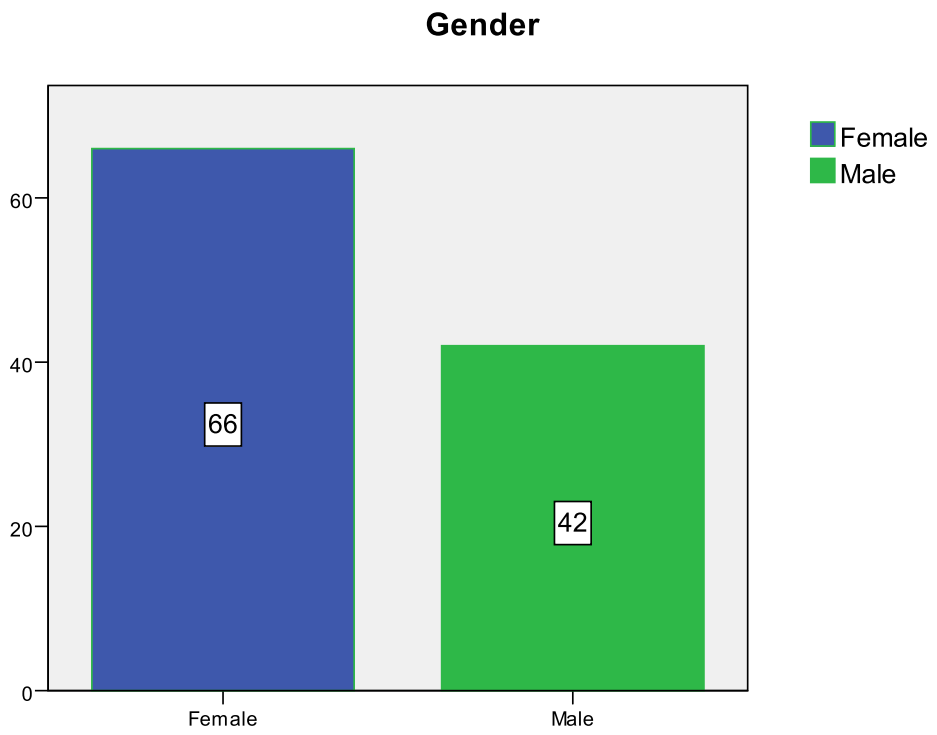


Table 6: Gender

Gender	Frequency	Percentage	Valid Percent	Cumulative Percent
Female	66	61.1	61.1	61.1
Male	42	38.9	38.9	100.0
Total	**108**	**100.0**	**100.0**	

Out of 108 respondents, 61.1% are female respondents and 38.9% are male respondents. Table 6 summarised the frequency, percentage, valid percentage and cumulative percent for gender.

Figure 13: Age group

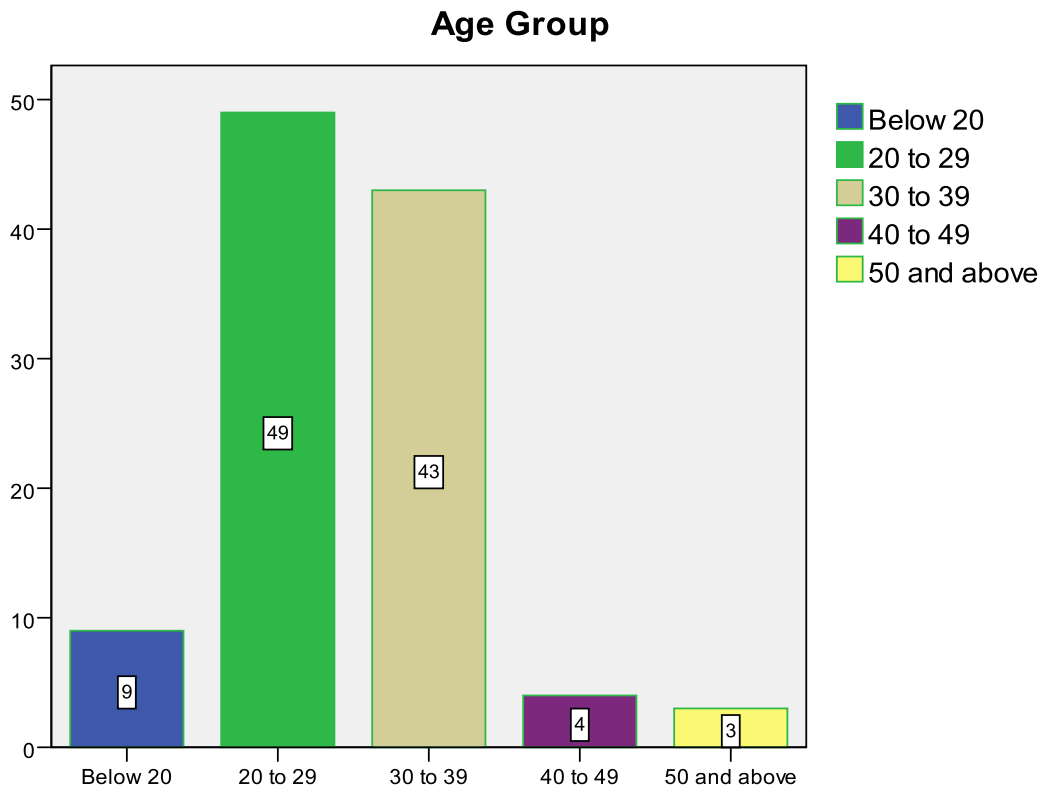


Table 7: Age group

Age Group	Frequency	Percentage	Valid Percent	Cumulative Percent
Below 20	9	8.3	8.3	8.3
20 to 29 years old	49	45.4	45.4	53.7
30 to 39 years old	43	39.8	39.8	93.5
40 to 49 years old	4	3.7	3.7	97.2
50 years old and above	3	2.8	2.8	100.0
Total	**108**	**100.0**	**100.0**	

Age group was categorised into five as shown in Table 7. There were 8.3% of respondents with the age of below 20 years old participated in this study. 45.4% respondents are in the age group of 20 to 29 years old. 39.8% respondents are in the age group of 30 to 39 years old. 3.7% respondents are in the age group of 40 to 49 years old. Only 2.8% of respondents are in the age group of 50 years old and above.

Figure 14: Education level

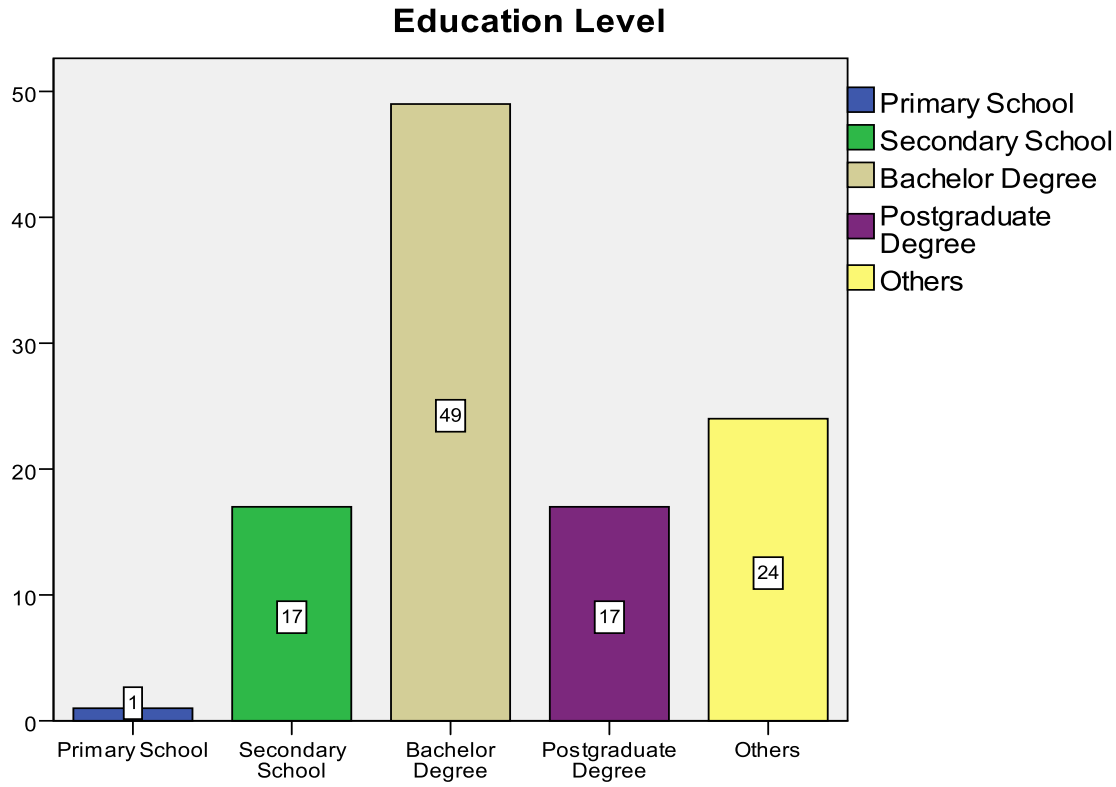


Table 8: Education level

Education Level	Frequency	Percentage	Valid Percent	Cumulative Percent
Primary school	1	0.9	0.9	0.9
Secondary school	17	15.7	15.8	16.7
Bachelor degree	49	45.4	45.4	62.1
Postgraduate degree	17	15.7	15.7	77.8
Others	24	22.2	22.2	100.0
Total	**108**	**100.0**	**100.0**	

Table 8 represents the frequency result of education level for 108 respondents whereby the respondents requested to indicate their current pursuing education level. 0.9% of the respondents' education level is up to primary school. 15.8% respondents reach the level of secondary school. 45.4% respondents hold a bachelor degree and 15.7% respondents graduated as postgraduate degree. 22.2% respondents indicate their education level as others.

Figure 15: Ethnicity

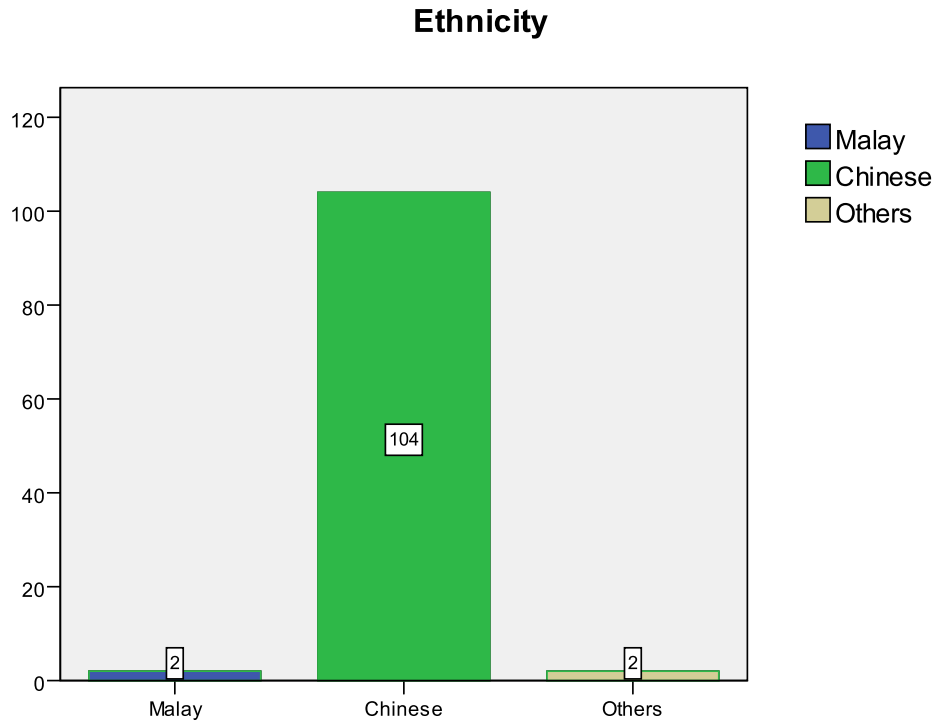


Table 9: Ethnicity

Ethnicity	Frequency	Percentage	Valid Percent	Cumulative Percent
Malay	2	1.9	1.9	1.9
Chinese	104	96.2	96.2	98.1
Indian	0	0	0	98.1
Others	2	1.9	1.9	100.0
Total	**108**	**100.0**	**100.0**	

Each of the Malay and other races contribute 1.9% in this survey data. The remainders 96.2% were contributed by Chinese. There was no data collected from Indian races.

Figure 16: Type of business / industry

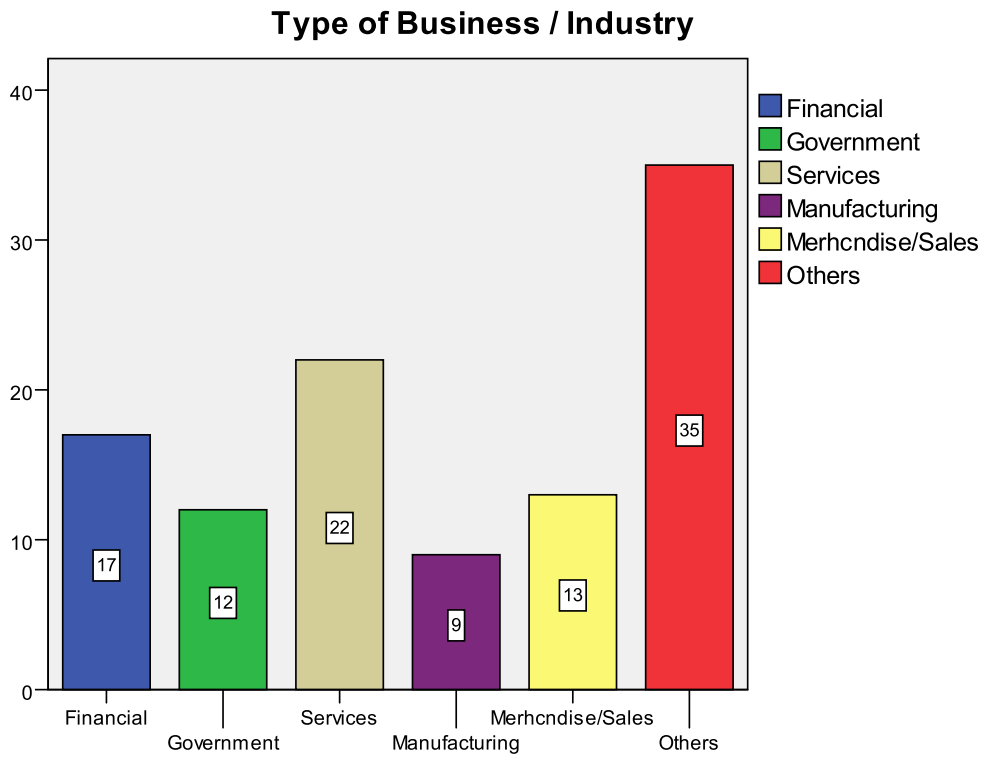


Table 10: Type of business / industry

Type of Business / Industry	Frequency	Percentage	Valid Percent	Cumulative Percent
Financial	17	15.7	15.7	15.7
Government	12	11.1	11.1	26.8
Services	22	20.4	20.4	47.2
Manufacturing	9	8.3	8.3	55.5
Merchandise / Sales	13	12.1	12.1	67.6
Others	35	32.4	32.4	100.0
Total	**108**	**100.0**	**100.0**	

Table 10 shown that 15.7% respondents are from financial industry, 11.1% from government sector, 20.4% from service industry, 8.3% from manufacturing industry, 12.1% from merchandise or sales business and 32.4% stated as others industry of business type.

Figure 17: Years in organistion

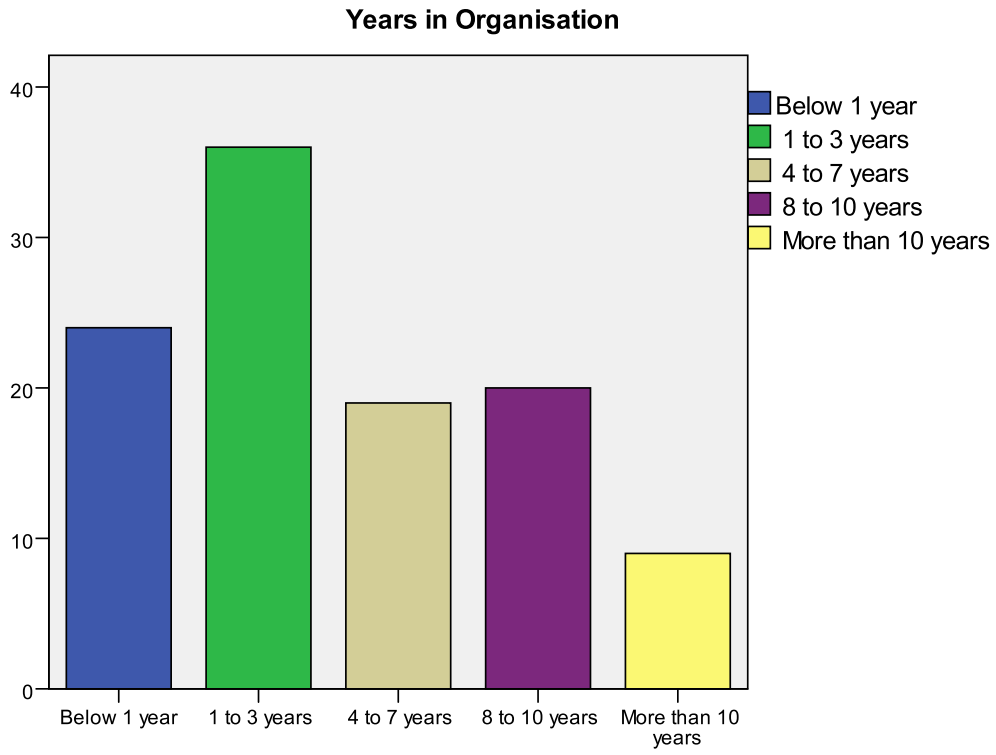


Table 11: Years in organisation

Years in Organisation	Frequency	Percentage	Valid Percent	Cumulative Percent
Below 1 year	24	22.2	22.2	22.2
Between 1 to 3 years	36	33.3	33.3	55.5
Between 4 to 7 years	19	17.6	17.6	73.1
Between 8 to 10 years	20	18.5	18.5	91.6
More than 10 years	9	8.4	8.4	100.0
Total	**108**	**100.0**	**100.0**	

Years in organisation of respondents classified into five main groups. 22.2% respondents are work less than a year, 33.3% work between one to three years, 17.6% work between four to seven years, 18.5% work between eight to 10 years and 8.4% work more than ten years in an organisation.

4.3.2 Knowledge Statements Statistics

Table 12: Knowledge statements statistics

Knowledge Statement	Mean	Standard Deviation	N
K1: I believe that my current working company has a written information security policy.	3.46	1.045	108
K2: I have read the information security policy sections that are applicable to my job.	3.20	0.993	108
K3: I understand the information security policy.	3.30	0.920	108
K4: I know what information security is.	3.46	0.990	108
K5: I know where to get a copy of the information security policy.	2.78	1.017	108
K6: I know what my responsibilities are regarding information security.	3.30	0.969	108
K7: I am informed of information security requirements to protect information.	3.32	1.022	108
K8: I know what the risk is when opening e-mails from unknown senders, especially if there is an attachment.	4.11	0.835	108
K9: I know how to use the anti-virus software to scan for viruses (e.g. when I download files from the Internet).	3.99	1.072	108
K10: When I leave my computer, I always lock the screen.	3.76	1.245	108
K11: At the end of the day, I ensure that there are no confidential documents left in my working area.	4.06	0.984	108

Throughout the mean score shown in Table 12, knowledge statement K5 carrying the lowest mean score of 2.78. Hence, it indicates that most of the respondents do not agree with the statement. K8 carrying the highest mean score of 4.11 while K9 (3.99) and K11 (4.06) mean score also indicated most of the respondents are agree with this three knowledge statements.

Table 13: Comparison between genders against knowledge statement statisctics

Gender vs Knowledge Statement				
Knowledge Statement	Gender	Number	Mean	P value*
K1: I believe that my current working company has a written information security policy.	Female	66	3.42	0.946
	Male	42	3.52	
K2: I have read the information security policy sections that are applicable to my job.	Female	66	3.18	0.200
	Male	42	3.24	
K3: I understand the information security policy.	Female	66	3.38	0.584
	Male	42	3.17	
K4: I know what information security is.	Female	66	3.62	0.141
	Male	42	3.21	
K5: I know where to get a copy of the information security policy.	Female	66	2.77	0.152
	Male	42	2.79	
K6: I know what my responsibilities are regarding information security.	Female	66	3.39	0.007*
	Male	42	3.14	
K7: I am informed of information security requirements to protect information.	Female	66	3.39	0.235
	Male	42	3.21	
K8: I know what the risk is when opening e-mails from unknown senders, especially if there is an attachment.	Female	66	4.12	0.058
	Male	42	4.10	
K9: I know how to use the anti-virus software to scan for viruses (e.g. when I download files from the Internet).	Female	66	3.82	0.996
	Male	42	4.26	
K10: When I leave my computer, I always lock the screen.	Female	66	4.06	0.000*
	Male	42	3.29	
K11: At the end of the day, I ensure that there are no confidential documents left in my working area.	Female	66	4.18	0.000*
	Male	42	3.86	

Independent samples T-test was used to test the significance differences among the gender of respondents against each of the knowledge statements. Results had been tabulated in Table 13. Knowledge statement 6, 10 and 11 have significant

difference between female and male. As highlighted in yellow color, it showed the P-value of 0.007, 0.000 and 0.000 which are smaller than 0.05 for knowledge statement 6, 10 and 11 respectively.

4.3.3 Conclusion Statements Statistics

Table 14: Conclusion statements' mean score

Conclusion Statement	Mean	Standard Deviation	Number
CON1: It has made me more worried about the information security policy.	3.34	0.959	108
CON2: I has made me more confident about my own knowledge on information security policy.	3.74	0.825	108
CON3: It has increased my awareness of information security policy as an issue.	3.88	0.758	108
CON4: It has made me realise I don't do as much as I thought.	3.35	1.035	108
CON5: It has made me realise I don't do as much as I could.	3.29	0.948	108
CON6: It is the same as before I taking this survey.	2.94	0.975	108

Overall, the mean score for conclusion statements are above value of 3. Even CON6 statement mean score (2.94) is the lowest, but it is merely reach the value of 3. It indicates that respondents were tend to agree with all the conclusion statements in the survey instrument.

Table 15: Comparison between genders against conclusion statement

Gender vs Conclusion				
Conclusion Statement	Gender	Number	Mean	P value*
CON1: It has made me more worried about the information security policy.	Female	66	3.23	0.276
	Male	42	3.52	
CON2: I has made me more confident about my own knowledge on information security policy.	Female	66	3.67	0.285
	Male	42	3.86	
CON3: It has increased my awareness of information security policy as an issue.	Female	66	3.80	0.565
	Male	42	4.00	
CON4: It has made me realise I don't do as much as I thought.	Female	66	3.27	0.998
	Male	42	3.48	
CON5: It has made me realise I don't do as much as I could.	Female	66	3.17	0.696
	Male	42	3.48	
CON6: It is the same as before I taking this survey.	Female	66	2.94	0.762
	Male	42	2.95	

All the P-value shown in Table 15 are greater than 0.05. It indicates that significant difference occurs between female and male opinions about information security governance upon the survey were done.

4.4 Multivariate normality

As quoted from Field (2005), the correlation coefficient value should be below 0.8 in order to avoid multivariate normality. It is important to test on the normality as to ensure that all data are compliance with statistical assumption of multivariate techniques.

4.4.1 Multicolinearity

Table 16: Test of multicolinearity

Variables	Training & Education	Trust	Employee Awareness	Ethical Conduct	Privacy
Education & Training	-				
Trust	0.664**				
Employee Awareness	0.495**	0.710**			
Ethical Conduct	0.357**	0.567**	0.659**		
Privacy	0.479**	0.557**	0.599**	0.693**	-

*Note: ** correlation is significant at 0.01 level (2-tailed)*

Table 16 shows the result of multicolinearity test among the independent variables. All correlation coefficient value shown are below 0.8.

4.5 Analysis of Independent Variables

Reliability test result in sub-chapter 4.2.2 (page 51) was applied towards 31 question statements which included all question statements under independent variables and dependent variable.

Table 17: Reliability analysis for independent variables

Independent Variable (IV)	Cronbach's Alpha	Number of Items / Statements	Statements
IV 1: Education and Training	0.744	5	1 to 5
IV 2: Trust	0.842	5	6 to 10
IV 3: Employee Awareness	0.843	6	11 to 16
IV 4: Ethical Conduct	0.725	6	17 to 22
IV 5: Privacy	0.851	5	23 to 27

Again, reliability test was carried for those independent variables individually. All Cronbach's alpha value shown in Table 17 are above the minimum Cronbach's alpha value of 0.60.

Table 18: Independent variables' mean score

Independent Variables	Mean	Standard Deviation	Number
Education and Training	3.4593	0.6495	108
Trust	3.7963	0.6511	108
Employee Awareness	3.9938	0.6114	108
Ethical Conduct	3.7531	0.6459	108
Privacy	3.6315	0.7759	108

As refer to Table 18, employee awareness score the highest mean compare to other independent variables which is 3.9938. Education and training gained the lowest mean score, 3.4593.

4.5.1 Comparison between genders

Table 19: Comparison between genders against independent variables

Gender vs Independent Variables				
Independent Variables	Gender	Number	Mean	P value*
Education and Training	Female	66	3.4273	0.007
	Male	42	3.5095	
Trust	Female	66	3.7818	0.160
	Male	42	3.8190	
Employee Awareness	Female	66	3.9470	0.140
	Male	42	4.0675	
Ethical Conduct	Female	66	3.6843	0.010
	Male	42	3.8611	
Privacy	Female	66	3.5515	0.110
	Male	42	3.7571	

*Note: *Equal variances assumed*

As highlighted in Table 19, P-value of education and training (0.007) and ethical conduct (0.010) are higher than 0.05. Thus, there is significant different between

female and male opinion in the education and training and ethical conduct issue regard to information security governance.

Whereas no significant different between female and male opinion in terms of trust, employee awareness and privacy issue relate to information security governance.

Table 20: Pearson correlation result for independent variables

Independent Variables	Pearson Correlation	P value*
Education and Training	0.600	0.000
Trust	0.643	0.000
Employee Awareness	0.621	0.000
Ethical Conduct	0.547	0.000
Privacy	0.606	0.000

*Note: *correlation is significant at 0.01 level (1-tailed)*

The strength of the linear relationship between two variables can be measured by using Pearson correlation analysis. The higher value of Pearson correlation generated, the stronger of influence between the tested variables. The positive or negative value generated indicates the direction or norm of influence between the two variables.

As stated in this study's hypothesis, all independent variables were expected to correlate with the employees' compliance on information security governance (dependent variable). Throughout the generated result shown in Table 20, all the independent variables have significant relationship with the dependent variable in this study as the P-value are smaller than 0.05.

Beside, all Pearson correlation value shown are positive which indicate that all independent variables having the direct influences toward the independent variable. Trust is tending to be the important component as it has the highest Pearson correlation value of 0.643.

4.6 Multiple Linear Regression

Multiple linear regression was adapted in this study to analyze the relationship between the employees' compliance on information security governance (independent variable) and five factors.

The best fit model for this study will be Model 5 as refer to the following Table 1. The R-value keeps increasing upon each and every additional independent variables add-in.

Table 21: Analysis of structure model

Model	R	R Square	Adjusted R Square	Std. Error of Estimate	R Square Change	F Change	Sig.
1	0.600[a]	0.360	0.354	0.61827	0.360	59.584	0.000[a]
2	0.683[b]	0.467	0.457	0.56675	0.107	13.555	0.000[b]
3	0.719[c]	0.517	0.503	0.54218	0.050	8.921	0.000[c]
4	0.733[d]	0.538	0.520	0.53293	0.021	7.143	0.000[d]
5	0.748[e]	0.559	0.537	0.52325	0.021	4.128	0.000[e]

a. Predictors: (Constant), Education and training
b. Predictors: (Constant), Education and training, Trust
c. Predictors: (Constant), Education and training, Trust, Employee awareness
d. Predictors: (Constant), Education and training, Trust, Employee awareness, Ethical conduct
e. Predictors: (Constant), Education and training, Trust, Employee awareness, Ethical conduct, Privacy
f. Dependent Variable: Compliance

4.6.1 Hypothesis Test

The significant value of Education and training and Privacy are both below 0.05 (P-value). Thus, this two components are significant and having relationship with Compliances.

Table 22: Multiple regression analysis

Regression Test	R2	F-value	Standardized Coefficient (β)	t-value	Sig.	Hypothesis Result
Compliances	0.559	25.837				
Education and Training			0.262	2.889	0.005	Supported
Trust			0.169	1.523	0.131	Not Supported
Employee Awareness			0.186	1.765	0.081	Not Supported
Ethical Conduct			0.085	0.835	0.406	Not Supported
Privacy			0.217	2.202	0.030	Supported

4.6.2 Multiple regression model

Multiple regression model for this study will be written as:-

Compliances = 0.559 + 0.262 Education and training + 0.217 Privacy

4.7 Summary

Analytic statistics were presented through out this chapter. Data had been coded for each of the questions for the convenience and easy access of data analysis. No missing data was found in this study as researcher had make up some setting in the online survey tool. Reliability result was at 0.941 which representing 94.1% of reliability for this study.

Descriptive analysis was used to analyze the demographics data. There are 66 female participants and 42 male participants for this study. The interpretations of demographic statistic were focus on the percentage instead of frequency as percentage is more presentable.

For those independent variables and dependent variables statistics, mean score were used to tack on the favorable opinion among participants. Beside, significant different were stated through the P-value generated. Additionally, researcher carried the sample t-test to seek the significant differences among female and male in the perception on all questions in the survey instrument. Lastly, a multiple linear regression model was formed.

CHAPTER 5

DISCUSSION AND CONCLUSION

5.1 Overview

This chapter is aim to present some the discussions related to the analyzed data and mainly to redefine the findings to answer the research questions stated in Chapter 1. Generally, the discussion were segregate into two main title which under 'Discussion on analysis result' and 'Key factors in compliance'.

In the title of 'Discussion on analysis result', employee's perception toward knowledge statement, perception upon survey done and perceptions among genders were discussed. On the other sub-chapter – Key factors in compliance, hypotheses summary and three factors which have no significant relationship with compliance were illustrated. Future study recommendations are suggested and a conclusion for this study will be presented at the end of this chapter.

5.2 Discussion on Analysis Result

5.2.1 Employee's Perception

In order to answer this study Research Question 1, the following discussion had been made. Top three and the lowest mean score knowledge questions were verified and further discussed in this sub-chapter as to illustrate the perception of employees toward their knowledge of information security governance.

Top three mean score ranking questions in knowledge questions are:

1. K8 (mean score = 4.11)

   "I know what the risk is when opening e-mails from unknown senders, especially if there is an attachment."

2. K11 (mean score = 4.06)

   "At the end of the day, I ensure that there are no confidential documents left in my working area."

3. K9 (mean score = 3.99)

   "I know how to use the anti-virus software to scan for viruses (e.g. when I download files from the Internet)."

As result, employees are more alert and have better knowledge towards information security. Thus, the awareness level among employees could consider had been increased. They are more aware and know how to utilise the tools in order to minimise the threats.

The lowest mean score question in knowledge questions:

1. K5 (mean score = 2.78)

   "I know where to get a copy of the information security policy."

Participants were not agree as they know where to get themselves a copy of the information security governance. Thus, employees should be informed as where and with who they manage to request for the copy of information security governance.

5.2.2 Key Factors that Affect Employee's Compliance

Table 23: Hypothesis acceptance

Hypothesis	Outcome
H1: Education and Training has significant relationship toward Compliance on information security governance.	Supported
H2: Trust has significant relationship toward Compliance on information security governance.	Not supported
H3: Employee Awareness has significant relationship toward Compliance on information security governance.	Not supported
H4: Ethical Conduct has significant relationship toward Compliance on information security governance.	Not supported
H5: Privacy has significant relationship toward Compliance on information security governance.	Supported

In this study, generated result shows that education and training has significant relationship toward compliance on information security governance and privacy also has significant relationship toward compliance on information security governance. However, trust, employee awareness and ethical conduct have no significant relationship toward compliance on information security governance.

Thus, this finding help researcher to answer the Research Question 2 as the key factors that affect employee's compliance on information security governance are education and training and privacy.

5.2.3 Opinion upon Survey Done

As stated in Research question 3, researcher would like to assess the employees' opinion on information security governance upon the survey was done. Thus the following discussion had been elaborated.

CON3 question was having the top mean score (3.88) among the rest of the questions in the conclusion section of questionnaire. This question statement is: *"It has increased my awareness of information security policy as an issue."*

Upon employees finish this survey, they feel that this survey instrument had indirectly alert and increase their awareness level toward information security governance. It seems to be one of the contributions of this study.

Participants were not agreeing to the CON6 statement whereby the mean score shown is 2.94. It stated that:*"It is the same as before I taking this survey."*

Employees were not agree that they feel the same as before this survey was took. Apparently, this question is a "trick" question which try to tackle the effort of participants when taking this survey. As in CON3 questions, participants were agree that their awareness level had been increased. Thus, they should not agree with this CON6 statement.

5.2.4 Perception among Genders

Refer to the t-test result, it shows that there is significant difference among female and male in the following questions statement:

1. K6 (P-value = 0.007)

   "I know what my responsibilities are regarding information security."

2. K10 (P-value = 0.000)

   "When I leave my computer, I always lock the screen."

3. K11 (P-value = 0.000)

   "At the end of the day, I ensure that there are no confidential documents left in my working area."

Female participants mean score is tends to "agree" and "strongly agree" while male participants mean score is fall on "neutral" and "agree" level. No further judgment on the perceptions among genders as it will need in-depth questions and analysis for the interpretation. Thus, it will be concluded that significant difference only occur in that three knowledge statements as the answer for this Research Question 4.

5.3 Limitation of the Study

One of the limitation found in this study was the sample size might too small as to represent the perception of all employees in Malaysia. Beside, from the statistics of ethnicity, more than 90% is Chinese. As for future research, more data should be collected and distributed more equally as for all citizen in Malaysia.

5.4 Future Research Recommendation

When comes to compliances on those corporate governance, those bigger organisations like multi-national company has no doubt and sure will take actions to develop, implement and keep reviewing on it. However, smaller organisations find it more difficult to implement comprehensive information security and training due to the lack of expertise within the organisation.

Furnell et. al. (2002) have suggested that computer based training (CBT) that is interactive and user-friendly may be a solution for smaller companies. They developed a prototype software security training tool for use by employees. This prototype was in its early phase of development and was being further tested and developed by the authors' research group.

Thus, future study might narrow down the scope and specify the sample as target on those small-medium enterprise (SME). Another reason behind as why is SME? Bigger organisations always involved internal auditor and external auditor but not for SME. Those, the extent of implementation for information security governance in SME will raise as a question.

5.5 Conclusion

Furnell et. al. (2002) quoted that information security is a critical issue for organizations which rely on the information technology. However, security policies are only effective and sustainable if employees know, understand and

accept them. Further discussed by Furnell et. al., the appropriate education, training and awareness is required within organisation.

The factor of education and training was supported by the result generated in this study. However, it shows that awareness has no significant relationship toward compliance on information security governance. Back to the result analyzed in knowledge statements, employees are aware and know about information security but not the place to obtain the copy. Thus, the findings which show that trust has no significant relationship with information security governance is logic.

Privacy has significant relationship with compliance on information security governance due to employees know that information is an asset for organization. In order to secure the information, privacy is important. Again, management should keep review the factors which influence the compliances toward information security governance.

REFERENCE

Anthens, G.H. (2005). Catches on. *Computerworld*, 39(44), 39-42.

Avison, D.E. (1993). Research in information systems development and the displine of information system. *In Proceeding of 4th Australian Conference on Information System*, Brisbance Old.

Besnard, D., & Arief, B. (2004). Computer security impaired by legitimate users. *Computers & Security*, 23, 253-264.

Borking, L. (2006). Without privacy standards no trust in and outside cyberspace. Retrived April 25, from http://www.prime-project.eu/events/standardisation-ws/slides/Withoutprivacynotrust-JohnBorking.pdf/file_view.

Brown, C.V., & Magill, S.L. (1994). Alignment of the IS functions with the Enterprise: Toward a model of antecedents. *Management Information Systems Quarterly*, 371-404.

Cardinali, R. (1995). Reinforcing our moral vision: Examining the relationship between unethical behavior and computer crime. *Work Study*, 44(8), 11-18.

CISA Review Manual. (2005). ISACA: Rolling Meadows.

COBIT (Control Objectives for Information and related Technology). 2004. *COBIT Security Baseline – An Information Security Survival Kit.* USA: IT Governance Institute.

Creswell, J.W. (2003). *Research design: Qualitative, quantitative and mixed methods approaches*. (2nd ed.). Thousand Oaks, CA: Sage.

Da Veiga, A. (2008). Cultivating and assessing information security culture. *Information Systems Mangement*. 24(2), 361-372.

Denning. D. E. (1999). Activism, Hacktivism and Cyberterrosism: The Internet as a Tool for Influencing Foreign Policy. *Network and Netwars: The Future of Terror, Crime and Military*, 239-288.

Dhamija, R., Tygar, J.D., & Hearst, M. (2006). Why Phishing Works. *In Proceedings of the SIGCHI conference on Human Factors in computing systems* (CHI '06), Rebecca Grinter, Thomas Rodden, Paul Aoki, Ed Cutrell, Robin Jeffried, and Gary Olson (Eds.). ACM, New York, NY, USA, 581-590.

Dojkovski, S., Lichtenstein, S., & Warren, S. (2006). Fostering information security culture in small and medium size enterprises: An interpretive study in Australia. Retrieved June 23, from http://csrc.Ise.ac.uk/asp/aspecis/20070041.pdf.

Downs, J.S., Holbrook, M., & Cranor, L.F. (2007). *Behavioral Response to Phishing Risk*. ACM International Conference Proceeding Series, ACM, Pittsburg, Pennsylvania, 26, 37-44.

Exhibit. Retrieved February 10, from http://www.computerhistory.org/internethistory/internet_history_80s.html

Field. A. (2005). *Discovering statistics using SPSS*. (2nd ed.). London: Sage.

Flowerday, S., & Von Solms, R. (2006). Trust an element of information security. *Security and Privacy in dynamic Environments.* Boston: Kluwer Academic Publisher.

Foong, C.L., & Bakar, H.J.A. (2013). Article: Personal Data Protection Act 2010. Retrieved January 20, from http://klbar.blogspot.com/2013/08/article-personal-data-protection-act.html.

Fowler, F.J., Jr. (2009). *Survey research methods*. (4th ed.). Los Angeles, CA: Sage.

Furnell, S., Gennatou, M., & Dowland, P. (2002). A prototype tool for information security awareness and training. *Logistics Information Management*, 15(5/6), 352-357.

Gaunt, N. (2000). Practical approaches to creating a security culture. *International Journal of Medical Informatics*, 60(2), 151-157.

Goh, G.G., Tan, N.L., Goh, C.Y., & Eze, U.C. (2008) Phishing: A Growing Challenge for Internet Banking Providers in Malaysia, *Communications of the IBIMA*, vol. 5.

Hair, J.F., Black, B.J., Babin, R.E., Anderson, R.L., & Tatham. (2005). *Multivariate data analysis*. (6th ed.). Englewood Cliffs, NJ: Pearson Prentice-Hall.

Hartmann, A. (1995). Comprehensive information technology security. A new approach to respond ethical and social issues surrounding information security in the 21st century. *IFLP TCLL 11th International Conference of Information Systems Security.*

Hawkins, K.W., Alhajjaj, S., & Kelley, S.S. (2003). Using COBIT to secure information assets. *The Journal of Government Financial Management*. 52(2), 22.

Herold, R. (2010). *Managing an information security and privacy awareness and training program* (2nd ed.). New York: Auerbach Publications.

Hellriegel, D., Slocum, J.W. (Jr), & Woodman, R.W. (1998). *Organizational behavior* (8th ed.), Cincinnati, OH: South-Western College Publishing.

Hirschheim, R., Schwarz, A., & Todd, P. (2006). A marketing maturity model for IT: Building a customer-centric IT organization. *IBM Systems Journal*, 45(1), 181-199.

IBM Business Consulting Services, (2006). Federal Information Security Management Act (FISMA) compliance solution: Improving management, operational, and technical controls over information, personnel, and physical security and privacy. Retrieved August 12, from http://www.03.ibm.com/industries/global/files/FISMA_Cutsheet_PS_0306 pdf.

Internet Usage in Asia. Retrieved February 10, from http://www.internetworldstats.com/stats3.htm

ISACA. (2008). Information Systems Audit and Control Association. Retrieved May 12, from http://www.isaca.org.

ISO. 2005. Information Technology Security Techniques. Code of Practice for Information Security Management. ISO/IEC 17799 (BS 7799-1: 2005).

ISO/IEC 17799 (BS 7799-1). (2005). Information technology security techniques. Code of practice for information security management.

Kehoe, D., Little, D., & Lyons, A. (1993). Strategic planning for information systems enhancement: IMS. *Journal of Manufacturing Technology Management*, 4(2), 29.

Knapp, K.J.,Marshall, T.E., Rainer, R.K., & Ford, F.N. (2006). Information security: management's effect on culture and policy. *Information Management & Computer Security*, 14(1), 24-36.

Kowalski, S. (1990). Computer ethics and computers abuse: A longitudinal study of Swedish university students. *IFLP TCLL 6th International Conference on Information Systems Security.*

Kruger, H.A. & Kearney, W.D. (2006). A prototype for assessing information security awareness. *Computers & Security*, 25, 289-296.

Lainhart IV, J. (2000). COBIT: A methodology for managing and controlling information and information technology risks and vulnerabilities. *Journal of Information Systems*, 14(1), 21.

Li, X., & Chandra, C. (2007). A knowledge integration framework for complex network management. *Industrial Management + Data Systems*, 107(8), 108(9).

Lungu, I. & Tabusca, A. (2010). Optimising Anti-Phishing Solutions Based on User Awareness, Education and the Use of the Latest Web Security Solutions, *Information Economica*, Vol. 14, No 2.

Martins, N. & Von der Ohe, H. (2003). Organisational climate measurement: New and emerging dimensions during a period of transformation. *South African Journal of Labour Relations*, 27(3), 41-59.

McAfee (2005). The threats within.

McCarthy, M.P., & Campbell, S. (2001). *Security Transformation*. New York: McGraw-Hill.

McFadzean, E., Ezingeard, J.N., & Birchall, D. (2007). Perception of risk and the strategic impact of existing IT on information security strategy at board level. *Online Information Review*, 31(5), 622.

Mcllwrath, A. (2006). *Information security and employee behavior*. Hampshire: Gower.

Mohamed, N.A., & Masket, R. (2007). Computer Crime: The Malaysian Approach, *Proceeding of the International Conference on Electrical Engineering and Informatics*. Institute Tecknologi Bandung, Indonesia, June 17-19.

Munir, A.B. (2007). Phishing in Asia: Are We Doing Enough?. *The 2007 ALIN Conference B.Public and Social Issues.*

MyCert Incidents Statistics. Retrieved May 2, from http://www.mycert.org.my/en/services/statistic/mycert/2013/main/details/914/index.html

Ohaya, C. (2006). *Managing Phishing Threats in an Organization*. Information Security Curriculum Development Conference, Proceedings of the 3rd annual conference on Information security curriculum development, ACM, Kennesaw, Georgia, p.159-161.

Orgill, G.L., Romney, G.W., Bailey, M.G and Orgill, P.M. (2004). *The Urgency for Effective User Privacy-education to Counter Social Engineering Attacks on Secure Computer Systems*. Information Technology Education (Formerly CITC), ACM, New York, USA, Salt Lake City, UT, USA, 177-181.

Pfleege, C.P. (1997). *Security in computing*. (2nd ed). New Jersey: Prentice Hall.

Phellas, C.N., Bloch, A., & Seale, C. (2011). Structured methods: Interviews, questionnaires and observation. Retrieved March 15, from http://www.sagepub.com/upm-data/47370_Seale_Chapter_11.pdf.

Puhakainen, P. (2006). A design theory for information security awareness. Retrieved January 13, from http://herkules.oulu.fi/isbn9514281144/isbn9514281144.pdf.

PWC (PricewaterhouseCoopers). 2004. Information Security Breaches Survey. Retrieved January 12, from http://www.dti.gov.uk/industry_files/pdf/ibs_2004v3.pdf.

Robbins, S. (2001). *Organizational behavior* (9th ed.), New Jersey: Prentice Hall.

Saint-German, R. (2005). Information security management best practice based on ISO/IEC 17799. *Information Management Journal*, 39(4), 60-62.

Saunders, M., Lewis, P., & Thornhill, A. (2012). *Research methods for business students* (6th ed.), UK: Pearson Education Limited.

Sekaran, U. (2003). *Research methods for business: A skill building approach*. (4th ed.), New York: John Wiley & Sons.

Sherwood, J., Clark, A., & Lynas, D. (2005). *Enterprise security architecture: A business driven approach*, Berkeley: CMP Books.

Smith, T., Koohang, A., & Behling, R. (2010). Understanding and prioritizing technology management challenges. *The Journal of Computer Information Systems*, 51(1), 91-98.

Stacey, T., & Helsley, R. (1996). Indentifying information security threats. *Information Systems Security*, 5(3), 50.

Stair, R.M., & Reynolds, G.W. (2010). *Information Systems*, 9th Ed., Canada: Course Technology Cengage Learning.

Swanson, R., & Holton, E. (2005). *Research in organizations: Foundations and methods of inquiry*. San Francisco, CA: Berrett-Koehler.

Tavakol, M. & Dennick, R. (2011). Internal Journal of Medical Education. Retrieved February 7, from http://ijme.net/archive/2/cronbachs-alpha.pdf.

Trim, P.R.J. (2005). Managing computer security issues: preventing and limiting future threats and disasters. *Disaster Prevention and Management*, 14(4), 493-505.

Van Niekerk, J.F. & Von Solms, R. (2010). Information security culture: a management perspective. *Computers & Security*, 29(4), 476-486.

Von Solms, R. (1997). Driving safely on the information superhighway. *Asian Libraries*, 6(3/4), 150.

Von Solms, R., & Von Solms, B. (2003). From policies to culture. *Computers and Security*, 23, 275-279.

Von Solms, S.H. (2005). Information security governance: compliance management vs. operational management. *Computers and Security*, 24(6), 443-447.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers and Security*, 23(3), 191-198.

Webb, N.M., Shavelson, R.J., & Haertel, E.H. (2006). Reliability coefficients and generalizability theory. Retrieved February 8, from http://www.stanford.edu/dept/SUSE/SEAL/Reports_Papers/methods_papers/G%20Theory%20Hdbk%20of%20Statistics.pdf.

Whitmore, J.J. (2001). A method for designing secure solutions. *IBM Systems Journal*, 40(3), 747-768.

Zulhuda, S. (2012). Personal Data Protection Act 2010 will be enforced from 01.01.2013-or so it was said.... Retrieved December 12, from http://sonnyzulhuda.com/2012/10/23/personal-data-protection-act-2010-will-be-enforced-from-01-01-2013/

UNIVERSITI TUNKU ABDUL RAHMAN

INFORMATION SECURITY (IS) GOVERNANCE: ASSESSING EMPLOYEES' KNOWLEDGE TOWARDS IS GOVERNANCE AND THE FACTORS AFFECTING EMPLOYEES' COMPLIANCE ON IS GOVERNANCE

Dear Respondent(s):

This research is being conducted with main objectives to better understand the knowledge of employees toward information security (IS) governance and the factors which will affect the employees' compliance on IS governance. The outcome of the finding will be useful for organizations in Malaysia in understanding the employees' current knowledge and compliance on IS governance in the organization, which will enable them to develop appropriate educational and awareness programmes for its employees in complying its IS governance.

The survey should take you about 10 minutes to complete. Please be assured that your responses will be kept strictly confidential and will be used only for the purposes of this research. To ensure anonymity, the responded survey forms will only be identified through an identification code on each form. Please return the completed questionnaire at your earliest convenience.

Your participation is highly appreciated and we thank you for your time and support.

If you have any questions about this study, you can contact the researcher(s) below:

Name of Researchers	e-mail Address
1. Chow Win Niy, Faculty of Accountancy and Management, UTAR.	*chowwn1@mail2.utar.edu.my*

Section 1: Demographic

1. Gender: ☐ Female ☐ Male

2. Age Group:
   ☐ Below 20
   ☐ 20 to 29 years old
   ☐ 30 to 39 years old
   ☐ 40 to 49 years old
   ☐ 50 years old and above

3. Education Level: (including currently pursuing, if any)
   ☐ Primary School
   ☐ Secondary School
   ☐ Bachelor Degree
   ☐ Postgraduate Degree
   ☐ Others

4. My ethnicity:
   ☐ Malay
   ☐ Chinese
   ☐ Indian
   ☐ Others

5. Type of business or industry:
   ☐ Financial
   ☐ Government
   ☐ Services
   ☐ Manufacturing
   ☐ Merchandise/Sales
   ☐ Other

6. Year(s) in organization:
   ☐ Below 1 year
   ☐ Between 1 to 3 years
   ☐ Between 4 to 7 years
   ☐ Between 8 to 10 years
   ☐ More than 10 years

Section 2: Information Security Culture

For the following statements, kindly rate your opinion by ticking on the relevant box based on the following scale:

1=Strongly Disagree, 2=Disagree, 3= Neutral, 4=Agree, 5=Strongly Agree.

A	Knowledge Statements	Strongly Disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly Agree (5)
1	I believe that my current working company has a written information security policy.	☐	☐	☐	☐	☐
2	I have read the information security policy sections that are applicable to my job.	☐	☐	☐	☐	☐
3	I understand the information security policy.	☐	☐	☐	☐	☐
4	I know what information security is.	☐	☐	☐	☐	☐
5	I know where to get a copy of the information security policy.	☐	☐	☐	☐	☐
6	I know what my responsibilities are regarding information security.	☐	☐	☐	☐	☐
7	I am informed of information security requirements to protect information.	☐	☐	☐	☐	☐
8	I know what the risk is when opening e-mails form unknown senders, especially if there is an attachment.	☐	☐	☐	☐	☐
9	I know how to use the anti-virus software to scan for viruses (e.g. when I download files from the Internet).	☐	☐	☐	☐	☐
10	When I leave my computer, I always lock the screen.	☐	☐	☐	☐	☐
11	At the end of the day, I ensure that there are no confidential documents left in my working area.	☐	☐	☐	☐	☐

Section 3: User Security Management

For the following statements, kindly rate your opinion by ticking on the relevant box based on the following scale:

1=Strongly Disagree, 2=Disagree, 3= Neutral, 4=Agree, 5=Strongly Agree.

D	Education and Training	Strongly Disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly Agree (5)
1	The contents of the information security policy were effectively explained to me.	☐	☐	☐	☐	☐
2	I believe there is a need for additional training to use information security controls in order to protect information.	☐	☐	☐	☐	☐
3	I believe the information security awareness initiatives are effective.	☐	☐	☐	☐	☐
4	I received adequate training to use the applications I require for my daily duties.	☐	☐	☐	☐	☐
5	The information security policy, procedures and guidelines clearly state what is expected of me to safeguard information.	☐	☐	☐	☐	☐
E	**Trust**	**Strongly Disagree (1)**	**Disagree (2)**	**Neutral (3)**	**Agree (4)**	**Strongly Agree (5)**
6	I believe that management communicates relevant information security requirements (e.g. what Internet usage is allowed, how to make backups, security usage of removable media such as USB's / PDA's) to me.	☐	☐	☐	☐	☐
7	I believe that Information Technology business unit implements information security controls (e.g. restricting access to secure areas, controlling access to computer systems, preventing viruses).	☐	☐	☐	☐	☐
8	I believe that IT business unit has adequate authority to ensure the implementation of information					

	security controls.					

E	Trust	Strongly Disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly Agree (5)
9	I believe that organization pays adequate attention to an information security strategy in order to protect information.	☐	☐	☐	☐	☐
10	I believe the IT business unit adequately assists in the implementation of controls to protect information.	☐	☐	☐	☐	☐
F	**Employee Awareness**	**Strongly Disagree (1)**	**Disagree (2)**	**Neutral (3)**	**Agree (4)**	**Strongly Agree (5)**
11	Information security is necessary in my business unit to protect information.	☐	☐	☐	☐	☐
12	The employees in our business unit perceive information security (e.g. sharing confidential information) as important to protect information.	☐	☐	☐	☐	☐
13	I am aware of the information security aspects relating to my job (e.g. when to change my password or which information I work with is confidential).	☐	☐	☐	☐	☐
14	It is necessary to protect information to achieve the business strategy of organization.	☐	☐	☐	☐	☐
15	There are adequate information security specialists/coordinators throughout my organization to ensure the implementation of information security controls.	☐	☐	☐	☐	☐
16	The information security controls implemented by organization support the business strategy.					
G	**Ethical Conduct**	**Strongly Disagree (1)**	**Disagree (2)**	**Neutral (3)**	**Agree (4)**	**Strongly Agree (5)**
17	I accept responsibility towards protection of information.	☐	☐	☐	☐	☐

18	I think it is important to regard the work I do as part of the intellectual property of company.	☐	☐	☐	☐	☐

G	Ethical Conduct	Strongly Disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly Agree (5)
19	I believe it is important to take care when talking about confidential information in public places.	☐	☐	☐	☐	☐
20	I believe that e-mail and Internet access are for business purposes and not personal use.	☐	☐	☐	☐	☐
21	I believe my colleagues comply with copy right laws.	☐	☐	☐	☐	☐
22	I believe that sharing of passwords should be used to make access to information easier.	☐	☐	☐	☐	☐
H	**Privacy**	**Strongly Disagree (1)**	**Disagree (2)**	**Neutral (3)**	**Agree (4)**	**Strongly Agree (5)**
23	I believe that third parties who have access to confidential information preserve the confidentiality thereof.	☐	☐	☐	☐	☐
24	There are clear directives on how to protect sensitive (confidential) client information.	☐	☐	☐	☐	☐
25	There are clear directives on how to protect sensitive (confidential) employee information.	☐	☐	☐	☐	☐
26	I believe that management keeps my private information (e.g. salary or performance appraisal information) confidential.	☐	☐	☐	☐	☐
27	I believe that the information I work with is protected adequately.	☐	☐	☐	☐	☐
I	**Compliance**	**Strongly Disagree (1)**	**Disagree (2)**	**Neutral (3)**	**Agree (4)**	**Strongly Agree (5)**
28	My business unit enforces adherence to the information security policy.	☐	☐	☐	☐	☐
29	Employees in our business unit	☐	☐	☐	☐	☐

	adhere to the information security policy.					
I	**Compliance**	**Strongly Disagree (1)**	**Disagree (2)**	**Neutral (3)**	**Agree (4)**	**Strongly Agree (5)**
30	Action should be taken against anyone who does not adhere to the information security policy (e.g. if they share passwords, give out confidential information of visit prohibited Internet sites).	☐	☐	☐	☐	☐
31	I should be held accountable for my actions if I do not adhere to the information security policy.	☐	☐	☐	☐	☐

Section 5: Conclusion

For the following statements, kindly rate your opinion by ticking on the relevant box based on the following scale:

1=Strongly Disagree, 2=Disagree, 3= Neutral, 4=Agree, 5=Strongly Agree.

How has completing this survey changed your opinion about information security policy?

I	**Items**	**Strongly Disagree (1)**	**Disagree (2)**	**Neutral (3)**	**Agree (4)**	**Strongly Agree (5)**
1	It has made me more worried about the information security policy.	☐	☐	☐	☐	☐
2	It has made me more confident about my own knowledge on information security policy.	☐	☐	☐	☐	☐
3	It has increased my awareness of information security policy as an issue.	☐	☐	☐	☐	☐
4	It has made me realise I don't understand as much as I thought.	☐	☐	☐	☐	☐
5	It has made me realise I don't do as much as I could.	☐	☐	☐	☐	☐

6	It is the same as before I taking this survey.	☐	☐	☐	☐	☐

WELL DONE! You have completed this survey!
Thanks so much for your participation.