ORIGINAL ARTICLE

Assessing drivers for organizational commitment towards the security controls implementation in the Malaysian online service in computer-based accounting system

1Dr Intan Salwani Mohamed, 2Izzatul Ussna Ridzwan, 3Dr Norzaidi Mohd Daud, 4Zakiah Baharin and 5Saidin Wan Ismail

1Faculty of Accountancy/Accounting Research Institute Universiti Teknologi MARA 40450 Shah Alam, Selangor Malaysia.
2College of Business Management and Accounting, UNITEK Sultan Haji Ahmad Shah campus, 26700 Bandar Muadzam Shah, Pahang, Malaysia.
3Faculty of Business Management/Accounting Research Institute/Institute of Business Excellence, Universiti Teknologi MARA 40450 Shah Alam, Selangor Malaysia.
4Faculty of Accountancy Universiti Teknologi MARA Johor 85009 Segamat Johor Malaysia.
5CITU, Universiti Teknologi MARA Johor 85009 Segamat Johor Malaysia.

Dr Intan Salwani Mohamed, Izzatul Ussna Ridzwan, Dr Norzaidi Mohd Daud, Zakiah Baharin and Saidin Wan Ismail; Accessing Drivers for Organizational Commitment Towards the Security Controls Implementation in the Malaysian Online Service in Computer-Based Accounting System.

ABSTRACT

The objective of this study is to determine the accessing drivers for organizational commitment towards security controls implementation in the Malaysian online service in computer based accounting system. Based on survey, data was collected from 63 firms in hotel/resort, financial and transportation industry, and suggested that firm size, managerial awareness, regulatory support, as well as vendor support were found to have a positive significant influence towards organizational commitment in security controls implementation. Also, the commitment to implement security controls first comes from the management itself especially senior and top management through managerial awareness as well as the need to safeguard the organization’s reputation. Moreover, regulatory support from government to encourage security controls implementation among organizations are important as it was proven that they have a significant influence towards organizational commitment in security controls implementation.

Key words: Organizational commitment, security controls, online service, computer based accounting system, Malaysia.

Introduction

The transformation from manual system to a computer-based system however, creates a new issue on how secure is the computer-based accounting system. The security of information has become one of the most important issues of computer-based accounting information system in most organizations, since their survival and success depends on a large extent on the confidentiality, accuracy, integrity, and availability of their critical and sensitive information. There are several surveys that have been conducted with the objective to investigate how far the cyber attacks affect the security system of most organizations. Among them are surveys from http://www.securelist.com (2010), which use an antivirus product, Karpersky Security Network (KSN) to detect malware attacks within systems; CSI Computer Crime and Security Threats (2010), which investigate how respondents felt about their own cyber-security situations within their organizations; and http://www.findwhitepapers.com (2010), which focuses on the level of cyber attacks in the financial services industry. All surveys show that information security ranked high in the list of critical success factors in most organizations. Therefore, protecting computer-based accounting information system against prospective security threats has become a very important issue (Abu Musa, 2006). Adequate protections must be put in place due to the computer crime especially for those companies that used online services as their major business transactions. It has become unavoidable problems in any organizations and no longer become a local problem. The security solutions as well cannot be viewed only from a national perspective, but also to be expanded throughout the geographical boundaries.

Corresponding Author: Associate Professor Dr Norzaidi Mohd Daud, Faculty of Business Management/Accounting Research Institute/Institute of Business Excellence, Universiti Teknologi MARA 40450 Shah Alam, Selangor Malaysia.
E-mail: zaidiuitm2000@yahoo.com
Given that the security controls is an important aspect that need to be explored in protecting accounting information system, the main issue that needs to be investigated is the relationship between factors under three characteristics that are technological characteristic (such as technology competence, web functionalities, accounting software usage and non-accounting software usage); organizational characteristic (such as firm size, managerial awareness and management beliefs); and environmental characteristic (such as regulatory support and vendor support) towards organizational commitment in security controls implementation specifically to those organizations that practicing online system in their everyday business operations.

The questions that arise in discussing the security of computer-based accounting system are:

i. Do factors under technology characteristics such as technology competence, web functionalities, accounting software usage, and non-accounting software usage have an effect on organizational commitment in security controls implementation?

ii. Do factors under organizational characteristics such as firm size, management awareness, and managerial beliefs have an effect on organizational commitment in security controls implementation?

iii. Do factors under environmental characteristics such as regulatory support and vendor support have an effect on organizational commitment in security controls implementation?

In answering the above questions, this study focused on whether these factors which are technology competence, web functionalities, accounting software usage and non-accounting software usage (technological characteristic); firm size, managerial awareness and management beliefs (organizational characteristic); and regulatory support and vendor support (environmental characteristic) affect organizational commitment on security controls implementation in computer-based accounting system. The findings of this study should be useful for organizations to evaluate the adequacy of their security controls implementation and will also create awareness among organizations on the importance of their commitment in security controls implementation.

Review of Literature:

Technology Competence and Organizational Commitment in Security Controls Implementation:

Ong and Ismail (2008) stated that information technology objects refer to availability of hardware, software, and personnel to support the performance of information technology operations. Bassellier et al. (2003) defined technology knowledge as the extent of technical knowledge regarding objects such as computer based systems. This knowledge is able to convert into competence when it is utilized or exploited. It also refers to the competency of personnel or employees that are responsible for managing the computer system. Thus, organizations must make sure that they have adequate technology facilities and knowledge to support their security system. Hypothesis 1 was developed to test the relationship between technology competences towards the organizational commitment in computer-based accounting system’s security controls implementation.

H1: Technology competence significantly influences organizational commitment in security controls implementation:

Web Functionalities and Organizational Commitment in Security Controls Implementation:

According to Shah and Murtaza (2005), resolving security and reliability issues are critical in the widespread adoption of online system. Moreover, Birman (2004) stated that, today, web services miss the functional reliability because the current models do not consider ‘real world’ issues and organizations failed to accept and adopt with rapid changes of technology. Therefore, top management need to see these issues more seriously as to make sure that the website of their organization is functioning and operating well as well as preventing attacks from cyber criminals. Thus, it is hypothesized as;

H2: Web functionalities significantly influence organizational commitment in security controls implementation:

Accounting Software Usage and Organizational Commitment in Security Controls Implementation:

Accounting software usage looks into the extent of various types of application software being used in the accounting department within organizations. Most important benefit of accounting software usage is it assists in eliminating many of most common errors made by humans, such as transposing numbers and using the wrong accounts. Thus, it contributes towards more quality financial information and increase the security of confidential information. Thus, accounting software usage is hypothesized as

H3: Accounting software usage significantly influences organizational commitment in security controls implementation.
Non-accounting Software Usage and Organizational Commitment in Security Controls Implementation:

The help of some additional applications software such as graphic programs (e.g. chart, graph and bar) and word processing (e.g. Microsoft Words and Text Maker) could give a better picture about the presentation of the financial statements for those who don’t have any accounting background and knowledge to understand the presentation of financial statements. Furthermore, it is used as a support or backup system for the accounting software in unpredictable situations. For organizations, by using these non-accounting software usages, most data, and information will be more manageable and structured before it is entered to the accounting software. Therefore, it is assumed that non-accounting software assist in providing more secure system in computer-based accounting system. The following hypothesis:

H4: Non-accounting software usage significantly influences organizational commitment in security controls implementation.

Firm Size and Organizational Commitment in Security Controls Implementation:

Firm size often being used in TOE Model as it is a good predictor of IT adoption in organizations (Lippert and Govindarajulu, 2006; and Mohamed et al. 2008). In this study, firm size is measured by examining the number of employees in the analysis’s unit. It was suggested in the European E-business Report that firm size can be grouped into four categories that are micro (0-9 employees); small (10-49 employees); medium (50-249 employees) and large (250 and above employees). According to Ma and Ratnasingam (2008), large firm may have more human and technological resources available to implement a high quality security system compared to small firm that is more interested in economic returns. Small firm size reflected constraints in their resource and do not ready to adopt new technology in terms of financial or facilities as they could not handle great risk. Thus, hypothesis 5 was developed to test the relationship between firm size and organizational commitment in security controls implementation.

H5: Firm size significantly influences organizational commitment in security controls implementation.

Managerial Awareness and Organizational Commitment in Security Controls Implementation:

Managerial awareness is very crucial as it is the key towards successful security management. Based on research done by Liao and Luo (n.d.), it was found that there is a lack of awareness concerning the security risks and employee education regarding prevention measures. Therefore, this study will examine whether managerial awareness has a relationship with organizational commitment in security controls implementation. To test the relationship, the following hypothesis is developed.

H6: Managerial awareness significantly influences organizational commitment in security controls implementation.

Management Belief and Organizational Commitment in Security Controls Implementation:

Management beliefs reflect the factors that influence managers to put commitment in security controls implementation and how top management acts to the needs for having a high quality security system in the computer-based system. This relates to their beliefs on the ease of use and usefulness of the security system in protecting their financial information. When they believed, they would change their perceptions regarding the benefits of adopting a good security system (Lippert and Govindarajulu, 2006). Therefore, it is hypothesized as;

H7: Management beliefs significantly influence organizational commitment in security controls implementation.

Regulatory Support and Organizational Commitment in Security Controls Implementation:

Regulatory support refers to governments’ role to encourage the needs of having quality security system by establishing laws and providing incentives. By having specific guidance in developing online or web site system as well as establishing laws to highlight the punishment for cyber criminals, it is assumed that the level of security controls will be increased. Therefore, the following hypothesis is developed.

H8: Regulatory support significantly influences organizational commitment in security controls implementation.

Vendor Support and Organizational Commitment in Security Controls Implementation:

Close relationship between vendor and customer organization influence positively the successful implementation of security software. Vendor’s role is not only to offer and supply the security software to their
customer organizations but also to transfer knowledge about the use of the software, understanding the business processes within the organization and recognizing best practice (Kouki et al. 2006). Thus, the following hypothesis

H9: Vendor support significantly influence organizational commitment in security controls implementation.

Theoretical Framework:

In this research, all variables were measured with the aim to answer the questions that were mentioned before. In this research, there are 10 variables, which are organizational commitment in security controls implementations (OCSCI), technology competence (TC), web functionalities (WF), accounting software usage (ASU), non-accounting software usage (NASU), firm size (FS), managerial awareness (MA), management beliefs (MB), regulatory support (RS) and vendor support (VS). These variables are categorized into dependent variable and independent variable as follow:

i. Dependent Variable:

This study only focuses on the direct relationship. Therefore, the dependent variable is organizational commitment in security controls implementation (OCSCI).

ii. Independent Variable:

The independent variables are the factors or drivers listed under each TOE characteristics. There are technology competence (TC), web functionalities (WF), accounting software usage (ASU), non-accounting software usage (NASU), firm size (FS), managerial awareness (MA), management beliefs (MB), regulatory support (RS), and vendor support (VS). All these independent variables have direct relationships with organizational commitment in security controls implementation (OCSCI) (Figure 1).

Fig. 1: Theoretical Framework for this Study, Sources: Developed for the Study.

Research Methodology:

In this study, focus was given to accounting department since this department involves with money transactions and because of that more security threats were expected to occur in this department. According to Bank Negara Malaysia (BNM) official website, until January 2011 there were 68 financial institutions registered under BNM which consists of commercial banks (23), Islamic banks (17), international Islamic banks (4), investment banks (15), other financial institutions (2), and money brokers (7). From 68 financial institutions, there are 35 banks that have website. As for hotels and tourism sectors, based on Malaysia Association of Hotels (MAH) directory, as at January 2011 there are 548 hotels which all have their own website. On the other hand, there are 108 transportation companies in Malaysia have their own official website. Altogether, the number of
populations that have website was 691. Based on this population, a sample was selected using random sampling. The sample size was determined according to a table provided by Sekaran (2003).

According to Sekaran (2003) a table “Determining Sample Size from a Given Population” provides a scientific guideline in determining the sample size. From the table, it states that for a population of 650, the sample size should be 242 and for a population of 700, the sample size should be 248. Since the population for this study is 691 which are nearest to 700, thus a sample size of 248 will be applied. This means that from the total of 691 organizations that constitutes the populations of interest, a sample of 248 organizations were selected randomly for the purpose of data collection.

This sample size fulfils the rule of thumb proposed by Roscoe (1975) which stated that an appropriate sample size should be larger than 30 and less than 500 for most researches. Roscoe (1975) further explained that if a sample size is too large (more than 500), it could lead to the case of committing Type II errors which means that the findings from the data examined could be reversed from rejected to accept. In this research, the sample size is 248 which are larger than 30 and less than 500. Therefore, type II errors were avoided.

Findings:

In this study, from 248 distributed questionnaires, 45 organizations responded through the postal method, 10 questionnaires were taken by hand and 8 organizations responded through e-mail. In total, there were 63 responses received which represented 25.40 percent of the returned sample size. Out of 63 responded questionnaires, 5 blank responses were found on the demographic information and the rest were on section B (drivers for organizational commitment in security controls implementation in computer-based accounting system) and section C (commitment in security controls in computer-based accounting system). As mentioned in previous section, the rule of thumb by Sekaran (2003) was used in dealing with blank responses.

According to Sekaran (2003), as long as the unanswered part of the questionnaire did not exceed 25 percent of the questionnaires, the data will still be included. For this study, blank responses did not exceed the 25 percent rule which means that all data was included. Based on Hussey and Hussey (1997), in order to avoid sample being bias for the mail distributed method, the responses rate received should exceed 10 percent. Since the response rate in this study was 25.40 percent, there was no sample bias and it represents the population. Based on the rules of thumb developed by Hair, Black, Babin, Anderson and Tatham (2006), the number of samples for sample size considerations should meet the minimum ratio of observations to variables is 5:1. It means that 5 observations are made for each independent variable and it should never fall below 5:1. For this study, there are 9 independent variables (5:9) which constitutes to 45 samples. Since this study collected 63 samples, thus it satisfied the rules of thumb by Hair et al. (2006). This rule of thumb was used since the response rate is small and may affect the validity of generalization of the results.

Demographic Profile of Respondents:

The selected respondents that answered the questionnaires were varied in demographics information such as industry sector, the starting year that their organization started doing business through web and the respondents’ position in their organization.

Table 1: Sample Characteristics (N=63).
Reliability Test:

Computing Cronbach’s Alpha is the most popular method uses to measure reliability in terms of consistency of the test (Sekaran, 2003). In Cronbach’s Alpha, the higher the coefficient leads to better measurement and higher confident. For reliability, the value should be close to one in order to indicate higher reliability. For this study, the minimum value of Cronbach Alpha will be based on the rule of thumb suggested by Hair, Anderson, Tatham and Black (2003), where .60 as the lowest level in accepting reliability. Table 2 shows the Cronbach’s Alpha score for each of the variables.

Table 2: Internal Consistency of the Construct.

<table>
<thead>
<tr>
<th>CONSTRUCTS</th>
<th>CRONBACH’S ALPHA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology Competence</td>
<td></td>
</tr>
<tr>
<td>TC1 (% employees use computer at work)</td>
<td>0.620</td>
</tr>
<tr>
<td>TC2 (% employees have IT qualifications)</td>
<td></td>
</tr>
<tr>
<td>Web Functionalities</td>
<td></td>
</tr>
<tr>
<td>WF1 (Website support service catalogue)</td>
<td>0.806</td>
</tr>
<tr>
<td>WF2 (Website support consumer customization)</td>
<td></td>
</tr>
<tr>
<td>WF3 Website support account management</td>
<td></td>
</tr>
<tr>
<td>WF4 (Website support registry of online community)</td>
<td></td>
</tr>
<tr>
<td>WF5 (Website applications electronically integrated with back-office system)</td>
<td></td>
</tr>
<tr>
<td>WF6 (Company databases electronically integrated with suppliers)</td>
<td></td>
</tr>
<tr>
<td>WF7 (Company databases electronically integrated with partners)</td>
<td></td>
</tr>
<tr>
<td>Accounting Software Usage</td>
<td>0.806</td>
</tr>
<tr>
<td>ASU1 (Audit Programs)</td>
<td></td>
</tr>
<tr>
<td>ASU2 (Financial Accounting Software)</td>
<td></td>
</tr>
<tr>
<td>ASU3 (Tax Application Software)</td>
<td></td>
</tr>
<tr>
<td>ASU4 (Management Accounting Software)</td>
<td></td>
</tr>
<tr>
<td>Non-Accounting Software Usage</td>
<td>0.662</td>
</tr>
<tr>
<td>NASU1 (Word Processing)</td>
<td></td>
</tr>
<tr>
<td>NASU2 (Spreadsheets)</td>
<td></td>
</tr>
<tr>
<td>NASU3 (Database Programs)</td>
<td></td>
</tr>
<tr>
<td>NASU4 (Graphics Programs)</td>
<td></td>
</tr>
<tr>
<td>Managerial Awareness</td>
<td>0.932</td>
</tr>
<tr>
<td>MA1 (Organization educates employees regarding securities issues in CBAS)</td>
<td></td>
</tr>
<tr>
<td>MA2 (Ensuring information are unchanged by unauthorized persons)</td>
<td></td>
</tr>
<tr>
<td>MA3 (Ensuring that a system is accessible upon demand by an authorized entity)</td>
<td></td>
</tr>
<tr>
<td>MA4 (Ensuring that a system is usable upon demand by an authorized entity)</td>
<td></td>
</tr>
<tr>
<td>MA5 (Ensuring that the responsible person could be detected for their actions)</td>
<td></td>
</tr>
<tr>
<td>Managerial Beliefs</td>
<td>0.899</td>
</tr>
<tr>
<td>MB1 (Security controls implementation benefit their technology investment)</td>
<td></td>
</tr>
<tr>
<td>MB2 (Security controls implementation protect sensitivity of company’s data)</td>
<td></td>
</tr>
<tr>
<td>MB3 (Security controls implementation protect their CBAS)</td>
<td></td>
</tr>
<tr>
<td>Regulatory Support</td>
<td>0.696</td>
</tr>
<tr>
<td>RS1 (Government provides good incentive for companies to implement security system)</td>
<td></td>
</tr>
<tr>
<td>RS2 (Secured transaction is required for government purchase)</td>
<td></td>
</tr>
<tr>
<td>RS3 (Secured transaction is required for online transactions)</td>
<td></td>
</tr>
<tr>
<td>Vendor Support</td>
<td>0.789</td>
</tr>
<tr>
<td>VS1 (Handle the hardware issues related to application)</td>
<td></td>
</tr>
<tr>
<td>VS2 (Handle the software issues related to application)</td>
<td></td>
</tr>
<tr>
<td>Organizational Commitment on Security Controls Implementation</td>
<td></td>
</tr>
<tr>
<td>AC1 (Access controls)</td>
<td>0.949</td>
</tr>
<tr>
<td>AC2 (Physical access)</td>
<td></td>
</tr>
<tr>
<td>AC3 (Restricting to data access)</td>
<td></td>
</tr>
<tr>
<td>NE1 (Physical resources)</td>
<td></td>
</tr>
<tr>
<td>NE2 (Environment)</td>
<td></td>
</tr>
<tr>
<td>BD1 (Resources protection)</td>
<td></td>
</tr>
<tr>
<td>DC1 (Warranted activity)</td>
<td></td>
</tr>
<tr>
<td>LA1 (Data prevention)</td>
<td></td>
</tr>
<tr>
<td>RLF1 (Means of recovery)</td>
<td></td>
</tr>
<tr>
<td>MSM1 (Security Program)</td>
<td></td>
</tr>
</tbody>
</table>

Firm size excluded due to single attribute of measurement (number of employees) Source: Computed data analysis.

For this study, one item has been deleted in order to increase the reliability statistics. The particular item is a sub question in “Technology Competence” that is TC3 (technology facilities used by organization prior to e-business implementation). Table 3 shows Cronbach’s Alpha of “Technology Competence” before TC3 was deleted. Table 4.7 shows that TC3 needs to be deleted to get the value of .620 which meet the minimum acceptable level of reliability.
Table 3: Reliability Statistics for Technology Competence.

<table>
<thead>
<tr>
<th>Reliability Statistics</th>
<th>Cronbach's Alpha</th>
<th>N of Items</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>.426</td>
<td>3</td>
</tr>
</tbody>
</table>

Source: Computed data analysis.

Table 4: Item-Total Statistics for Technology Competence.

<table>
<thead>
<tr>
<th>Item-Total Statistics</th>
<th>Scale Mean if Item Deleted</th>
<th>Scale Variance if Item Deleted</th>
<th>Corrected Item-Total Correlation</th>
<th>Cronbach's Alpha if Item Deleted</th>
</tr>
</thead>
<tbody>
<tr>
<td>TC1</td>
<td>.003813</td>
<td>1.262</td>
<td>.513</td>
<td>-.227</td>
</tr>
<tr>
<td>TC2</td>
<td>-.041074</td>
<td>1.746</td>
<td>.231</td>
<td>.377</td>
</tr>
<tr>
<td>TC3</td>
<td>-.011934</td>
<td>2.155</td>
<td>.077</td>
<td>-.620</td>
</tr>
</tbody>
</table>

Source: Computed data analysis.

**Standard Regression Analysis:**

Under the regression analysis, the relationship between the independent variables from technological characteristics (such as technology competence, web functionalities, accounting software usage, and non-accounting software usage), organizational characteristics (such as firm size, managerial awareness and management beliefs) and environmental characteristics (such as regulatory support and vendor support) towards organizational commitment in security controls implementation will be measured. As each dependent and independent variables had several sub-questions, therefore data will be measured using mean. For this study, standard regression analysis used the significant level α = .05. This means that the conclusion that was made based on statistical inference will be correct at a confidence level of 95 percent and there is only 5 percent chance that the conclusion will be wrong.

Table 5: The Relationship between Dependent and Independent Variables.

<table>
<thead>
<tr>
<th>Model Summarya</th>
<th>Model</th>
<th>R</th>
<th>R Square</th>
<th>Adjusted R Square</th>
<th>Std. Error of the Estimate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>.784*</td>
<td>.615</td>
<td>.550</td>
<td>.46135</td>
</tr>
</tbody>
</table>

a. Predictors: (Constant), TC, ASU, VS, FS, MB, RS, NASU, MA

b. Dependent Variable: OCSCI

Key:
TC: Technology Competence
WF: Web Functionalities
ASU: Accounting Software usage
NASU: Non-Accounting Software Usage
FS: Firm Size
MA: Managerial Awareness
MB: Management Beliefs
RS: Regulatory Support
VS: Vendor Support
OCSCI: Organizational Commitment on Security Controls Implementation

Source: Computed data analysis

Based on Table 5, R square is .615. The R Square indicates that 61.5% of the variation in the organizational commitment in security controls implementation (OCSCI) is explained by four significant independent variables that are regulatory support (RS), vendor support (VS), management beliefs (MB) and firm size (FS). The balance of 38.5% is explained by other factors such as technology competence (TC), web functionalities (WF), accounting software usage (ASU), non-accounting software usage (NASU), and managerial awareness (MA). The ANOVA table (Table 6) shows that the model is significant, with the F-value of 9.404.

Table 6: ANOVA Table.

<table>
<thead>
<tr>
<th>ANOVAa</th>
<th>Model</th>
<th>Sum of Squares</th>
<th>DF</th>
<th>Mean Square</th>
<th>F</th>
<th>Sig.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Regression</td>
<td>18.014</td>
<td>9</td>
<td>2.002</td>
<td>9.404</td>
<td>.000*</td>
</tr>
<tr>
<td></td>
<td>Residual</td>
<td>11.281</td>
<td>53</td>
<td>.213</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td>29.295</td>
<td>62</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

a. Predictors: (Constant), TC, ASU, VS, FS, MB, RS, NASU, MA

b. Dependent Variable: OCSCI

Key:
TC: Technology Competence
WF: Web Functionalities
ASU: Accounting Software usage
NASU: Non-Accounting Software Usage
FS: Firm Size
MA: Managerial Awareness
MB: Management Beliefs
Hypotheses Testing and Discussion of Findings:

This research used standard regression analysis to evaluate the direct influence of independent variables (technology competence, web functionalities, accounting software usage and non-accounting software usage (technological characteristics); firm size, managerial awareness and management beliefs (organizational characteristics); and regulatory support and vendor support (environmental characteristics) towards organizational commitment in security controls implementation. In order to examine the relationship between these factors and organizational commitment in security controls implementation, nine hypotheses have been developed to be tested. Table 7 shows the result and findings of the relationship between the independent and dependent variables and the summary of hypotheses testing.

Table 7: Summary of Hypothesis Testing.

<table>
<thead>
<tr>
<th>Hypothesis</th>
<th>Relationship</th>
<th>Beta</th>
<th>T ratio</th>
<th>Sig</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1</td>
<td>TC→OCSCI</td>
<td>-.120</td>
<td>-1.174</td>
<td>.245</td>
<td>Rejected</td>
</tr>
<tr>
<td>H2</td>
<td>WF→OCSCI</td>
<td>-.063</td>
<td>- .635</td>
<td>.528</td>
<td>Rejected</td>
</tr>
<tr>
<td>H3</td>
<td>ASU→OCSCI</td>
<td>.097</td>
<td>.984</td>
<td>.329</td>
<td>Rejected</td>
</tr>
<tr>
<td>H4</td>
<td>NASU→OCSCI</td>
<td>-.078</td>
<td>-.706</td>
<td>.483</td>
<td>Rejected</td>
</tr>
<tr>
<td>H5</td>
<td>FS→OCSCI</td>
<td>.209</td>
<td>2.059</td>
<td>.044</td>
<td>Accepted</td>
</tr>
<tr>
<td>H6</td>
<td>MA→OCSCI</td>
<td>.106</td>
<td>.629</td>
<td>.532</td>
<td>Rejected</td>
</tr>
<tr>
<td>H7</td>
<td>MB→OCSCI</td>
<td>.338</td>
<td>2.312</td>
<td>.025</td>
<td>Accepted</td>
</tr>
<tr>
<td>H8</td>
<td>RS→OCSCI</td>
<td>.334</td>
<td>2.873</td>
<td>.006</td>
<td>Accepted</td>
</tr>
<tr>
<td>H9</td>
<td>VS→OCSCI</td>
<td>.269</td>
<td>2.765</td>
<td>.008</td>
<td>Accepted</td>
</tr>
</tbody>
</table>

Dependent Variable: Organizational Commitment on Security Controls Implementation

As a whole, looking at drivers for security implementation in computer-based accounting system, regulatory support (β = .334) is found to have the most significant influences towards organizational commitment in security controls implementation follows by vendor support (β = .269) management beliefs (β = .338) and firm size (β = .209). The details of analysis for each of the hypothesis are further discussed next.

Technology Competence:

This study suggested that there is no significant relationship between technology competence and organizational commitment in security controls implementation (p > .05, β = -.120) (Table 7). Therefore, H1 is rejected. This finding is consistent with Saad (2006) which stated that security system that can be achieved through technical means is limited. He further stated that security decisions that were based on technology competence and employees’ technical expertise were relevant in the past but due to certain factors such as financial implications in implementing and maintaining the security system, organizations’ today choose to take risks than to invest in security system. Technology competence also seems to have no relationship with organizational commitment because of management has no trust in doing online business, thus they do not concentrate in implementing technology facilities (Walter and Ritter, 2005). Shah and Murtaza (2005) also stated that organizations’ nowadays failed to accept and adopt with rapid changes of technology. Furthermore, the reason why technology competence does not influence organizational commitment is due to the fact that technology itself cannot provide all answers to security problems (Saad, 2006).

Web Functionalities:

The result shows that there is no significant relationship between web functionalities and organizational commitment in security controls implementation (p > .05, β = -.063) (Table 7). Therefore, H2 is rejected. This is
supported by Birman (2004) which stated that, today, web services miss the functional reliability because the current models do not consider ‘real world’ issues and organizations failed to accept and adopt with rapid changes of technology. The reason why web functionalities do not have relationship with organizational commitment in security controls implementation could also due to the web functionalities’ problems it selves. The problems can result in missed opportunity, missing accounting data, unacceptable and incorrect accounting data, and problems of having duplicate accounting data which leads to more complicated and adding burden to organizations’ management compared to normal business operations (Wiliam, 1997).

**Accounting Software Usage:**

Accounting software usage has no relationship with organizational commitment in security controls implementation. The analysis demonstrate that accounting software usage do not effect organizational commitment in security controls implementation ($p > .05, \beta = .097$) (Table 7). Thus, hypothesis 5 (H5) is rejected. The result from this study is similar to Intan Salwani et al. (2005). Intan Salwani and Norzaidi (2005) stated that accounting software such as UBS Accounting, One Write plus DOS Package and Peachtree has their own security controls and this accounting software does not permit unauthorized person to open or use the system. The security systems of this particular accounting software for example, required users to enter the password in order to get the accounting information stored. Since accounting software has its own security controls, management took this advantage as an opportunity for them to let go in giving commitment towards the security issues in accounting software usage.

**Non-Accounting Software Usage:**

After conducted the analysis, the result in Table 7 shows that there is no significant relationship between non-accounting software usage and organizational commitment in security controls implementation ($p > .05, \beta = -.078$). Therefore, H4 is rejected. This result is contrary with Mohamed et al. (2009) which found that non-accounting software has a positive relationship with organizational commitment in security controls implementation. This might be due to the reason that these types of applications’ software do not provide any controls in safeguarding the information stored and nowadays, each industry have their own unique professional software such as Ezee FrontDesk Hotel Software for tourism industry, Polaris Software for financial industry and Trucking Software for transportation industry. Therefore, management does not focused on the security controls for non-accounting software usage as they have better software that suit the unique environment of the particular industry.

**Firm Size:**

This study finds that firm size has positive significant influence towards organizational commitment in security controls implementation ($p < .05, \beta = .209$) (Table 7). This means that when firm size goes up by 1 standard deviation, organizational commitment in security controls implementation goes up by .209 standard deviations. Thus, hypothesis 5 (H5) is not rejected. The result of this finding is contrary to Intan Salwani and Norzaidi (2005); and Intan Salwani et al. (2009). These two previous researches discovered that firm size had negative relationships towards organizational commitment in security controls implementation. For this study, one possible reason on the positive relationship between firm size and organizational commitment in security controls implementation might be related to theories by Ma and Ratnasingam (2008) which stated that large firm may have more human and technological resources available to implement a quality security system compared to small firm that is more interested in economic returns. Small firm size reflected constraints in their resource and do not ready to adopt new technology in terms of financial or facilities as they could not handle great risk. This means that the larger the firm is, the more resources available to implement a quality security system and vice versa. Furthermore, the larger the firm is, the larger the Accounting Department which may result in more complicated transactions and a lot of financial resources are needed to overcome it. This demonstrates the positive significant relationship between firm size and organizational commitment in security controls implementation. Another reason might be due to the needs to maintain a good reputation especially for large and well-known organizations. Study done by Salehi et al. (2009) stated that large firms have a reputation to safeguard and they will make sure that quality security system will be adopted.

**Managerial Awareness:**

The result shows that there is no significant relationship between managerial awareness and organizational commitment in security controls implementation ($p > .05, \beta = .106$) (Table 7). Therefore, H6 is rejected. The reason why there is no relationship between managerial awareness and organizational commitment in security
controls implementation could be based on research done by Liao and Luo (n.d.) and Norzaidi et al (2011) which found that there is a lack of management’s awareness concerning the security risks and employee education regarding prevention measures. It could also due to the reason that most of top management does not have serious concerns about the security system in the organizations because they leave the responsibilities to the IT and Accounting Department.

Management Beliefs:

Management beliefs have a positive significant relationship with organizational commitment in security controls implementation (p < .05, β = .338) (Table 7). Therefore, when management beliefs go up by 1 standard deviation, organizational commitment in security controls implementation goes up by .338 standard deviations. Thus, hypothesis 7 (H7) is not rejected. This positive relationship might be due to the management beliefs on the ease of use and usefulness of the security system in protecting their financial information. The more the top management beliefs in the importance of having quality security systems, the more commitment they will give to implement it. Thus, when they beliefs in the usefulness of having the security system, they would changed their perceptions regarding the overall benefits of adopting such security system (Lippert and Govindarajulu, 2006).

Regulatory Support:

Regulatory support shows the most significant positive relationship with organizational commitment in security controls implementation (p < .05, β = .334) (Table 7). This means that when regulatory support goes up by 1 standard deviation, organizational commitment in security controls implementation goes up by .334 standard deviations. Thus, hypothesis 8 (H8) is not rejected. This finding is opposite with Intan Salwani et al. (2008) which found that there is no relationship between regulatory support and e-commerce. This can be due to the different population of interest for this study that are financial, tourism and transportation sectors compared to tourism sector by Intan Salwani et al. (2008) as the main focus of the study. The reason for this relationship might come from the awareness of the government to provide sufficient legal protection, clear business law and to safeguard organizations confidential information as it might include government’s private information. Furthermore, it has become a trend for organizations nowadays, where they will only act, follow, and behave according to rules and laws as they are bound to do so. Organizations tend to avoid in giving commitment if there are not bound in any regulations to do such actions. Thus, by having a clear rules and strong support from the government, organizations tend to give more commitment towards security controls implementation.

Vendor Support:

Vendor support has a positive significant relationship with organizational commitment in security controls implementation (p < .05, β = .269) (Table 7). This demonstrates that when vendor support goes up by 1 standard deviation, organizational commitment in security controls implementation goes up by .269 standard deviations. Therefore, hypothesis 9 (H9) is not rejected. This positive relationship is supported with theories by Kouki et al. (2006) that close relationship between vendor and the customer organization influence positively the successful implementation of security software. Most of organizations tend to stick to the same vendor for such a long time thus they manage to build close relationships with one another. According to Kouki et al. (2006) and Norzaidi and Intan Salwani (2010), by having close relationships, the vendor’s role is not only to offer and supply the security software to their customer organizations but the most important duty and responsibility is to transfer knowledge about the use of the software, understanding the business processes within the organization and recognizing best practice.

Based on the research findings, this study meets the general objective that is to assess the drivers for organizational commitment towards the security controls implementation in computer-based accounting system specifically in Malaysia online services. All the three specific objectives are answered as follow:

i. In determining to which technology characteristics’ factors such as technology competence, web functionalities, accounting software usage, and non-accounting software usage do give impact towards the organizational commitment in the implementation of security controls, the finding found that none of the variables have significant influence towards the organizational commitment in the implementation of security controls. This means that technology competence, web functionalities, accounting software usage, and non-accounting software usage were not good predictors of organizational commitment in security controls implementation.

ii. The research’s finding shows that organizational characteristic’ factors such as firm size and management beliefs are good predictors as they have influence towards the organizational commitment in the
implementation of security controls. However, managerial awareness has no relationship and is not good predictors to organizational commitment in security controls implementation.

iii. In determining whether environmental characteristics’ factors such as regulatory support and vendor support do give an impact on the organizational commitment in the implementation of security controls, the finding of this research found that both regulatory support and vendor support have a significant positive relationship with organizational commitment in the implementation of security controls. This show that regulatory support and vendor support are good predictors to organizational commitment in security controls implementation.

**Contribution of This Study to Bridge the Gaps of Knowledge:**

By conducting this research, the objectives to bridge the gaps of knowledge on the following issues have been achieved.

i. This study contributes in minimizing the gap by looking not only at the security controls implementation issues but also the organizational commitment towards the security controls implementation in online services focusing on the services industries.

ii. This research has contributes in minimizing the gap of publish work done by developing countries such as Malaysia in organizational commitment in security controls implementation.

iii. By using the TOE Model in investigating the relationship between factors on security controls and organizational commitment in security controls implementation, this study contributes in adding up one more research and bridging the gap by increasing the number of researches that used TOE Model Malaysia.

**Implications of the Study:**

Based on the research findings, firm size, managerial awareness, regulatory support, and vendor support were found to have a positive significant influence towards organizational commitment in security controls implementation. This study has revealed that the commitment to implement security controls first comes from the management itself especially senior and top management through managerial awareness as well as the need to safeguard the organization’s reputation. At the same time, regulatory support from government to encourage security controls implementation among organizations are important as it was proven that they have a significant influence towards organizational commitment in security controls implementation. This could be done by developing laws together with policies and strategic directions as it assists in encouraging the use of such technologies in a secure environment. Besides, support from vendor is also crucial as it encourages and motivates organizations towards having more secured systems. Therefore, this study have highlighted that there are four factors that could drive the security controls implementation in computer-based accounting system.

**Recommendations:**

Recommendations that can be derived from the findings of this research is that, organizations that practice and use computer-based accounting system in their business operations should evaluate their adequacy of commitment in security controls implementation. Focus should be given to the four factors that drive the security control implementations which are firm size, managerial beliefs, regulatory support, and vendor support as they have significant influences to the computer-based accounting system. Security controls is very important since it assist in ensuring the integrity of financial statement as well as increasing the quality of financial information that will be used by managers in making decision.

**References**


Online Available: Retrieved February 5, 2011 from https://www.javelinstrategy.com

Online Available: Retrieved February 9, 2011 from www.findwhitepapers.com


