Customer’s Perception Towards Information Security in Internet Banking System in Malaysia

1Associate Professor Dr Norzaidi Mohd Daud, 2Nor Izad Mamud and 3Sabrina Abd Aziz

1Faculty of Business Management/Accounting Research Institute/Institute of Business Excellence Universiti Teknologi MARA 40450 Shah Alam, Selangor, Malaysia.
2Arshad Ayud Graduate Business School Universiti Teknologi MARA 40450 Shah Alam, Selangor, Malaysia.
3Arshad Ayud Graduate Business School Universiti Teknologi MARA 40450 Shah Alam, Selangor, Malaysia.

Abstract: This research examines the customer’s perception towards information security in internet banking systems or I-system. A total of 330 respondents were selected from the simple random sampling. The results indicated that the confidentiality and privacy significantly influence the customer’s perception towards information security. Meanwhile for integrity, availability and verification is not a predictor of customer’s perception towards information security. The findings of this study create awareness to bank on the importance of customer’s perception towards information security in I-system and how bank could improve upon their internet banking system. This study is perhaps one of the first to address all the variables in a single setting in relation to perceived information security by customer.

Key words: Information security, customer’s perception, internet banking system, Malaysia

Background of Study:

Internet banking has become an important service for the bank (Sarrafiaghdam, 2003). To ensure the successfulness of internet banking, bank must provide a robust security system (Norzaidi et al., 2011; Intan Salwani and Norzaidi et al, 2009) to convince customers to use the internet banking system as the alternative from traditional banking. Research is needed to analyze the customer’s perception towards information security in internet banking. Furthermore, with a weak security system in internet banking result the customers not convinced with the system and wasted the bank investment for the system (Hutchinson and Warren, 2001). The convenience of internet banking to undertake the banking transaction outside of the working hours and from anywhere indeed become of the customer preference (Sohail and Shaikh, 2008). In order to secure I-system 24 hours, the system must be equipped with high security system together with regular test to ensure its reliability. Usage of a number of security technologies such as encryption, firewalls, automatic log-off and monitoring tools is part of the security measure that can be employed by bank for I-system (Banking Info, 2010). Moreover, installation of system to detect and disable attacks from hackers is highly needed nowadays (Hutchinson and Warren, 2001). With a security of information in place, it will convince the customers in choosing I-system as their internet banking provider.

Furthermore, the management of bank has experienced difficulties during the proposal for the internet banking system (I-system) to Bank Negara Malaysia (BNM). This is due to the weak security to secure the information in the system. BNM also highlighted, the increasing innovative cyber criminals in the area of internet banking has position a stringent rules for the internet banking system implementation (Banking Info, 2010). It is very important for bank to address the security issue in order for the customers to fully utilize I-system system. Therefore, bank must adherence to the highest protection to safeguard the private and confidential data of the customers. Customers are still reluctant to use I-system as their worries lies on the security of information especially their financial information. Customer’s preference for internet banking has been rising due to the conveniences, such as possibility to undertake banking transactions outside of banks hours and from anywhere as long as internet access is available (Sohail and Shaikh, 2008). This makes the availability of the system to customers when it is needed. Consequently, there is an urge for bank to increase
the efficiency and also to tighten up the security of the internet banking. In common with many other surveys
that point out that information security being the number one concern for customers (Ernst and Young, 1999),
this uptake is being challenged by concerns of potential customers towards the security and privacy of internet
banking transactions as well as confidentiality regarding the processing of personal information (Hutchinson
and Warren, 2001). Moreover, customers nowadays are concerned on the problem of spam in damaging the
internet banking services. Therefore, bank must adhere to the highest protection to safeguard the private
and confidential data of the customers. Although I-system is a new internet banking services, the information
security is the common inherent risk to bank. Controls are crucial in order to mitigate these risks for the
customer to feel secured while using I-system. By understanding the customer’s perception, it will help in
increasing the usage of I-system.

However there is still much to discover regarding the issue of rejection in using technology (Norzaidi et.al,
2008b) and the factors that contribute to the perceived information security. Most of the survey by bank is
looking at the customer’s feedback without taking into consideration of others resources such as articles and
journals that are useful to indicate the customer’s perception towards information security in I-system. It is
widely documented that from the insufficient information security in internet banking would cause usage to
be lower than expected (Norzaidi and Intan Salwani, 2007a; Norzaidi and Intan Salwani, 2010). As a result,
company suffers with lost in the technology investment.

Many preceding researches focusing on customer perception towards information security and most of them
is done in the western countries (Hutchinson and Warren, 2001), (Sohail and Shaikh, 2008). Thus, most of the
studies are looking at the broad information security. This study is importance because it is looking at the
specific information security within the I-system system and further analyzes the factors that may influence
the customer perception towards information security. Confidentiality, Integrity and Availability (CIA) triad
is meaningful to investigate the perception towards information security. To further justify the customers
perception, verification and privacy play an important part since without it, customers is reluctant to use I-
system. Notwithstanding the above, no prior studies have incorporated and tested these factors in a single
setting.

Thus, the objective of the study is to investigate the customer perception towards information security in
internet banking systems (I-system). The specific objectives are as follows:
1. To determine whether confidentiality has a relationship with perceived information security.
2. To investigate whether integrity has a relationship with perceived information security.
3. To examine whether availability has a relationship with perceived information security.
4. To study whether verification has a relationship with perceived information security.
5. To explore whether privacy has a relationship with perceived information security.

The next section reviews pertinent literatures that have garnered theoretical and practical support.

Review of Literature:
Confidentiality and Perceived Information Security:
Confidentiality in this study is defined as preventing the disclosure of information to unauthorized individuals
or systems. According to Sarrafiaghdam (2003), confidentiality plays an important role in ensuring the process
of information through identification. Thus, confidentiality is the core principles of information security (Parker,
2002) which partially determines the perceived information security by customers. The study by Sarrafiaghdam
(2003) show that confidentiality is a significant predictor to the perceived information security and
Sarrafiaghdam believed that there were fits between confidentiality and information security for the customers
to be convince in using internet banking system. It is necessary for maintaining the confidentiality of the
personal information against unauthorized reading, copying, or disclosure using encryption mechanisms
(Ratnasingam, 2002). Hence confidentiality should have a relationship with perceived information security, the
following hypothesis is constructed:
H1. Confidentiality has a relationship with perceived information security.

Integrity and Perceived Information Security:
Integrity on the other hand is defined as transaction accuracy and assurance that the transactions are done
in system application have not been altered or deleted undetectably. Sarrafiaghdam (2003) conducted a survey
on 132 respondents in Klang Valley. Based on the statistical analysis, they found that integrity is an important
element in the internet banking system that must be in place in order to foster the security system. As per CIA
triad, integrity is violated when a message is actively modified in transit. Information security systems typically provide message integrity in addition to data confidentiality. Thus, customers rely on the integrity of such system in doing transaction via internet banking. Web services use reliable messaging to enforce integrity ensuring that the message was only sent once, thus avoiding duplicate messages (Snell, 2001). Thus, the following proposition thus ensues:

**H2. Integrity has a relationship with perceived information security.**

**Availability and Perceived Information Security:**

Availability defines as an authorization mechanisms assuring transactions are sent and received without interruption when needed (Ratnasingam, 2002). For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information must be maintain with high security controls to protect it from outsiders. Ensuring availability also involves preventing denial of service attacks. According to Sarrafiaghdam (2003), availability is consider as the important element in the information security and fit to study the effect towards customer’s perception in the internet banking. Furthermore, the study shows significant relationships between availability and perceived information security. In the Internet banking environment, the availability is an important factor that affects the perceived information security that transacted online via the Web, thus leads to the following proposition:

**H3. Availability has a relationship with perceived information security.**

**Verification and Perceived Information Security:**

Although there are studies examined the verification in information system, (Hutchinson and Warren, 2003), there is no study identified to examine the relationships between verification and perceived information security by customers. Verification defines as the accuracy of the domain name can be ascertained, proving that customers are transacting with the actual internet banking system. For our study, verification depicture as crucial in each transaction through internet banking and there must be verification through the customers i.e. the used of transaction authorisation code (TAC) in internet banking application. The reasons provide good base for this study to measure the relationships between verification and perceived information security. The inherent lack of implicit identity verification that can be linked with an electronic transaction means that a spurious Web site could easily be created. When relating with Internet banks customers may make the mistake in the domain name, “www.Citibank.net” instead of “www.Citibank.com” or may misspell Citibank with a “y” instead of an “i” as in Citybank (Chellappa and Pavlou, 2001). There have been many instances of sites that have gained advantage from such typographical errors (Sullivan, 2000). In this sense, the customer wants verification that the accuracy of the domain name can be ascertained, proving that they are transacting with the actual internet bank, the following hypothesis is proposed:

**H4. Verification has a relationship with perceived information security.**

**Privacy and Perceived Information Security:**

The issues of privacy and information security are not new and have always been the greatest proportion of literature by other researchers. There even a study by Smith et. al (1996), that further break down the privacy variable into collection, improper access, errors and secondary use to test the relationships with risk and trust. Privacy in this study defines as the ability of the internet banking system to ensure the secrecy of personal and customers account information. Moreover, Sheng et.al (2008) also highlighted that privacy affect customer’s behavior in doing transactions over the internet. It is therefore interesting for the current study to ascertain the relationship between the privacy and perceived information security. Customers who adopt electronic financial services are more likely to perceive problems related to loss of privacy, as the internet seemingly allows other people to access their information easily (Jones, 2000). Customers do not always believe privacy policies will keep customer information confident (Gerrard and Cunningham, 2003). This argument leads to the following proposition:

**H5. Privacy has a relationship with perceived information security.**

Figure 1 shows the framework developed to depict the relationships between the variables. The next section presents the methodology used in this study.
Fig. 1: Research framework.

**Methodology:**

**Data and Sources of Data:**

The survey instruments used in this research is questionnaire. This questionnaire is designed based on seven-point Likert scales where “1= strongly disagree” to “7= strongly agree”. It has two sections, the first section of the questionnaire is about respondents’ demographic information, in which is designed to collect related data from the respondent such as age, education, gender, and in addition some questions intended to investigate more in terms of experience and involvement with Internet Banking and financial literacy of the participants. The second section of the questionnaire of Likert scales to investigate on the research variables. It comprised six items on confidentiality, integrity and availability whereby four items was taken from Donn Parker (2002) and two items was taken from Sarrafiaghdam (2008), six items on verification whereby all was taken by Hutchinson and Warren (2001), six items on privacy whereby four items was taken from Smith et.al., (1996) and balance of two items was taken from Attaran and VanLaar (1999) and six items on perceived information security which was taken from Sarrafiaghdam (2008).

**Sample of Study:**

The questionnaires are distributed to a targeted population of the bank customers situated in Kuala Lumpur. The targeted population was estimated two thousand of I-system users. The customers were then selected due to their experience of using I-system services as this is very crucial in determining the customer perception towards I-system services. The respondent first were asked if they have experience in using I-system prior to answers the survey questions. A simple random sampling procedure was used to select for the respondents. This sampling procedure has the least bias and offers the most generalizability (Sekaran, 2003).

As per Sekaran and Bougie (2010), if the population is amounting to 2,000, the sample size of 322 is required. In addition, Krejcie and Morgan (1970) had provide a table that can simplified the size decision in order to determine whether a good decision model being used. About 330 questionnaires were distributed to the customers of I-system services in the selected branches namely at Jalan Melaka and Jalan Tunku Abdul Rahman. The selection of these branches due to the convenient location in the middle of Kuala Lumpur and high number of customers doing the banking transaction. Out of 330 questionnaires distributed, 106 (33 percent) responses were obtained. It is considered to be high to represent of the population studied as Sekaran (2003), indicate that an analysis should obtain at least 30 percent responses. Furthermore, in order to avoid sample bias, response rate should be more than 10 percent (Roscoe, 1975). Moreover the results obtained can be generalize (Sekaran 2003).

After the data is collected, it been analyzed using the statistical software SPSS. Usage of the statistical techniques was according to commonly accepted research assumptions where appropriate. A pilot test on 20 samples was used to test goodness of measures in the form of reliability. The test is important to ensure that the questionnaire that is developed to measure a particular concept is indeed accurately measuring the variable and in fact is actually measuring the concept that is set out to measure (Sekaran, 2006). Cronbach’s Alpha is used to determine the internal reliability of the multi items variable. The reliability of measure indicates the extent to which it is without bias (error free) and thus ensures consistent measurement across the various items in the questionnaire. Better results of reliability for the questionnaire if the Cronbach’s Alpha gets to 1.0. In general, reliabilities less than 0.60 are considered poor, those in the 0.70 range, acceptable and those over 0.80 good (Sekaran, 2006). The pilot test with 20 respondents obtained 0.978 Cronbach’s Alpha. Other test used includes regression analysis to trace the mutual influence between the independent variables being measured. The following approaches have been taken in order to come up with the prospected results:

- Entering data into SPSS and preparation of data file. It involves with conversion of raw data source to a usable data file for analysis.
• Reliability test; Cronbach’s alpha as a correlation coefficient.
• Descriptive statistics; to explore the data collected and to summarize and describe the data. The demographics are useful to make some general observations about the data collected.
• Data transformation; to set the items by using the ‘Compute’ command in order to group 36 items into 6 research constructs which are Perceived Information Security, Confidentiality, Integrity, Availability, Verification and Privacy. Six items on confidentiality, integrity and availability whereby four items was taken from Donn Parker (2002) and two items were taken from Sarrafiaghdam (2008), six items on verification whereby all was taken by Hutchinson and Warren (2001), six items on privacy whereby four items was taken from Smith et.al., (1996) and balance of two items was taken from Attaran and VanLaar (1999) and six items on perceived information security which was taken from Sarrafiaghdam (2008).
• Multivariate assumptions; assessment of Normality of data using statistic (Skewness and Kurtosis) ways to explore the assumption of normality.
• Regression Analysis; to examine the relationship between the constructs.

Findings:
Descriptive Statistics:
The questionnaires are randomly distributed to a total of 330 respondents and 106 respondents answered the questionnaire, which provide a response rate of 33 percent. It is considered to be high to represent of the population studied as Sekaran (2003) indicated that an analysis should obtained at least 30 percent responses. Furthermore, in order to avoid sample bias, response rate should be more than 10 percent (Roscoe, 1975). Moreover the results obtained can be generalized (Sekaran 2003). Below are the explanations of the demographic characteristics of survey respondents. The demographic characteristics of 106 respondents are analyzed by six categories, namely years of using internet banking, gender, age group, highest level of education, current position in company and income level.

It suggested that the entire respondents have experience in using internet banking. Therefore, the respondents have sufficient knowledge and experience in dealing with internet banking. About 43 percent of the respondents have between one to two years experience in using internet banking. Meanwhile 33 percent of the respondents have more than two years of experience and 24 percent of the respondents have been using less than one year of internet banking. Moreover, the majority (42 percent) of the respondents aged 20 to 30 years old and the least percentage (3 percent) of the respondents aged more than 50 years old. The rest of the respondents are aged less than 20 by 9 percent, aged between 31 to 40 years old by 33 percent and aged between 41 to 50 years old by 14 percent. Also, the majority of the respondents are degree holders by 49 percent. The rest of the respondents are with diploma education (27 percent), secondary education (15 percent), master and above education (8 percent) and primary education (1 percent). In addition, 43 percent are executive, 23 percent are clerk, 13 percent are manager, 9 percent are professionals, 7 percent are students and 5 percent are others.

Normality Analysis:
In general, statistic test requires the population of the sample data comes from a normal distribution (Shapiro and Wilk 1965) (Royston, 1982). This is because without normality requirement, the results of the analysis will not be accurate. Hence, it is very important to ensure that the normality test and assumptions are satisfied. Methods of assessing normality can be divided into numerical and graphical. Examples of numerical method are Kolmogorov Smirnov statistic and Shapiro Wilk statistic. By using this method, it allows us to make objective judgment on the normality. Normally the experienced researcher used this method as they can make subjective judgment from their experience. Also, this method is highly used by the researchers that have least experience in interpreting the graphical method. Nevertheless, the numerical method is not sensitive enough for the low sample sizes. It is also overly sensitive to a larger sample size. On the other hand, the graphical method such as histograms, stem and lead plots and boxplots has some advantage over the numerical method. The graphical method allows good judgment about the data when the numerical tests are over or under sensitive. Yet, this method is lacking of objectivity. For this research, with less experience in interpreting the graphical method, the numerical method is chosen to test the normality of the data. In specifically, the Shapiro-Wilk test is used as the sample size between 7 and 2000 (Shapiro and Wilk 1965) (Royston, 1982).

The result from the Shapiro-Wilk test is shown in Table 1 above. According to Shapiro and Wilk (1965), if the sig. value of Shapiro-Wilk is greater than 0.05, the data is considered to be normal. But if the sig. value is below 0.05, then the data significantly deviate from the normal distribution. The results as per table 2 are above 0.05 and this indicated that the data is normally distributed.
Table 1: Tests of Normality.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Shapiro-Wilk Statistic</th>
<th>df</th>
<th>Sig.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perceived Information Security</td>
<td>0.980</td>
<td>106</td>
<td>0.115</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>0.976</td>
<td>106</td>
<td>0.052</td>
</tr>
<tr>
<td>Integrity</td>
<td>0.980</td>
<td>106</td>
<td>0.118</td>
</tr>
<tr>
<td>Availability</td>
<td>0.981</td>
<td>106</td>
<td>0.143</td>
</tr>
<tr>
<td>Verification</td>
<td>0.988</td>
<td>106</td>
<td>0.451</td>
</tr>
<tr>
<td>Privacy</td>
<td>0.979</td>
<td>106</td>
<td>0.087</td>
</tr>
</tbody>
</table>

a. Lilliefors Significance Correction

Table 2: Skewness and Kurtosis for Normality Test.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Minimum Statistic</th>
<th>Maximum Statistic</th>
<th>Mean Statistic</th>
<th>Std. Deviation Statistic</th>
<th>Skewness Statistic</th>
<th>Std. Error</th>
<th>Kurtosis Statistic</th>
<th>Std. Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability Confidentiality</td>
<td>3.00</td>
<td>7.00</td>
<td>4.7484</td>
<td>0.75636</td>
<td>0.267</td>
<td>0.235</td>
<td>0.207</td>
<td>0.465</td>
</tr>
<tr>
<td>Integrity Perceived Privacy Verification</td>
<td>6.50</td>
<td>6.50</td>
<td>6.70</td>
<td>0.73921</td>
<td>0.173</td>
<td>0.235</td>
<td>-0.428</td>
<td>0.465</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>3.00</td>
<td>4.7862</td>
<td>4.8758</td>
<td>0.79318</td>
<td>0.173</td>
<td>0.235</td>
<td>0.173</td>
<td>0.465</td>
</tr>
<tr>
<td>Integrity</td>
<td>3.00</td>
<td>4.9387</td>
<td>4.9387</td>
<td>0.78387</td>
<td>0.012</td>
<td>0.235</td>
<td>-0.538</td>
<td>0.465</td>
</tr>
<tr>
<td>Perceived Information Security</td>
<td>7.00</td>
<td>7.00</td>
<td>5.0550</td>
<td>0.79805</td>
<td>0.046</td>
<td>0.235</td>
<td>-0.400</td>
<td>0.465</td>
</tr>
<tr>
<td>Privacy</td>
<td>3.00</td>
<td>7.00</td>
<td>4.9843</td>
<td>0.76412</td>
<td>0.046</td>
<td>0.235</td>
<td>-0.312</td>
<td>0.465</td>
</tr>
</tbody>
</table>

The normality test was further conducted by looking at the skewness and kurtosis. To measure the degree of departure from symmetry of a distribution is known as skewness, while kurtosis measure the degree of flatness or peakedness of a distribution. According to Hair et al., (1998), the level of Skewness more than two and Kurtosis more than three indicate non normality. For skewness test, positive values indicate a positive skew while negative values indicate a negative skew. If the value of skewness is zero if the distribution is normal. Meanwhile for Kurtosis, positive values indicate a distribution that is peaked while negative values indicate a distribution that is flatter. A zero value of kurtosis also indicates that the distribution is normal. Based on table 4.8 below, the values of skewness for all the variables are positive and below than two. This indicated that the data is normal and have a positive skew. On the other hand, kurtosis tests shown are below three which indicate that the data is normal. For availability variable, the figure shown that the distribution is peaked, while the negative figures for confidentiality, integrity, perceived information system, privacy and verification variables indicated flat distribution. As a whole, the figures for skewness and kurtosis shown that the data is normal.

Reliability Analysis:

It is very important to study the properties of measurement scales and the items that compose the scales. Usage of SPSS software was done in order to ensure the variables in the model are reliable. Most commonly used reliability test is Cronbach’s Alpha Index. This is due to the interpretation as a correlation coefficient and it is ranges from 0 to 1. Besides that, using the Cronbach’s Alpa Index can determine whether the questionnaire is reliable and the data can be used for further analysis (Hair et al., 1998). Further analysis can only be done is the Cronbach’s Alpha Index test is passed (Nunally, 1967). According to Hair et al (1998), the acceptance level of Cronbach Alpha Index should exceed 0.7. Table 3 shows the result of reliability statistics which is 0.922 and it’s highly consistent.

Table 3: Reliability Statistics

<table>
<thead>
<tr>
<th>Cronbach’s Alpha</th>
<th>Cronbach’s Alpha Based on Standardized Items</th>
<th>N of Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.922</td>
<td>0.922</td>
<td>6</td>
</tr>
</tbody>
</table>

Table 4: Details of Reliability Statistics

<table>
<thead>
<tr>
<th>Variable</th>
<th>Corrected Item-Total Correlation</th>
<th>Squared Multiple Correlation</th>
<th>Cronbach's Alpha if Item Deleted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perceived Information Security</td>
<td>0.754</td>
<td>0.684</td>
<td>0.911</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>0.801</td>
<td>0.716</td>
<td>0.905</td>
</tr>
<tr>
<td>Integrity</td>
<td>0.784</td>
<td>0.635</td>
<td>0.907</td>
</tr>
<tr>
<td>Availability</td>
<td>0.777</td>
<td>0.675</td>
<td>0.908</td>
</tr>
<tr>
<td>Verification</td>
<td>0.805</td>
<td>0.695</td>
<td>0.904</td>
</tr>
<tr>
<td>Privacy</td>
<td>0.743</td>
<td>0.596</td>
<td>0.913</td>
</tr>
</tbody>
</table>
Correlation Analysis:

According to Jahangir and Begum (2008), Pearson correlation is used to examine the relationship between the variables. If the value of correlation coefficient range from 0.10 to 0.29 is considered weak. Meanwhile the value range from 0.30 to 0.49 is considered medium and from 0.50 to 1.0 is considered strong according to Wong and Hiew (2005). There is also an indicator that the correlation coefficient should not go beyond 0.8 to avoid multicollinearity (Field, 2005). Multicollinearity occurs when two or more variables in the model are correlated and provide redundant information. It is often confusing and lead to misleading results. As indicated in table 5, correlation coefficient are less than 0.8, therefore it is assumed that multicollinearity problem exists in this research.

Table 5: Correlation Analysis

<table>
<thead>
<tr>
<th></th>
<th>Perceived Information Security</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Availability</th>
<th>Verification</th>
<th>Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perceived Information Security</td>
<td>Pearson Correlation 1</td>
<td>.784**</td>
<td>.653**</td>
<td>.549*</td>
<td>.597**</td>
<td>.665**</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Pearson Correlation .784**</td>
<td>1</td>
<td>.728**</td>
<td>.641**</td>
<td>.663**</td>
<td>.596**</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>.000</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Integrity</td>
<td>Pearson Correlation .653**</td>
<td>.728**</td>
<td>1</td>
<td>.684**</td>
<td>.691**</td>
<td>.593**</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.000</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Availability</td>
<td>Pearson Correlation .549**</td>
<td>.641**</td>
<td>.684**</td>
<td>1</td>
<td>.781**</td>
<td>.660**</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.000</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Verification</td>
<td>Pearson Correlation .597**</td>
<td>.663**</td>
<td>.691**</td>
<td>.781**</td>
<td>1</td>
<td>.685**</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.000</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Privacy</td>
<td>Pearson Correlation .665**</td>
<td>.596**</td>
<td>.597**</td>
<td>.660**</td>
<td>.685**</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Sig. (2-tailed)</td>
<td>0.000</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
</tbody>
</table>

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

There are strong relationships between all the variables as the respective correlation is above 0.5. Furthermore, the sig (2-tailed) values are less than 0.05 indicated that there are statistically significant correlations between variables. Therefore, if any of the variable increases or decreases, the other variables also increases or decreases.

Regression Analysis:

Regression analysis is a constructive statistical technique that can be used to analyze the associations between a set of independent variables and a single dependent variable (Hair et al., 2005). Multiple regressions is used to examine the relationship between perceived information security, integrity, availability, verification and privacy.

Table 6: Regression Summary for Perceived Information Security

<table>
<thead>
<tr>
<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>0.837*</td>
<td>0.684</td>
<td>0.668</td>
<td>0.43601</td>
</tr>
</tbody>
</table>

Predictors: (Constant), Privacy, Integrity, Availability, Confidentiality, Verification

Table 7: ANOVA Table for Perceived Information Security

<table>
<thead>
<tr>
<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>41.058</td>
<td>5</td>
<td>8.212</td>
<td>43.195</td>
</tr>
<tr>
<td></td>
<td>Residual</td>
<td>19.011</td>
<td>100</td>
<td>0.190</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td>60.069</td>
<td>105</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Predictors: (Constant), Privacy, Integrity, Availability, Confidentiality, Verification

Table 8: Coefficients’ Table for Perceived Information Security

<table>
<thead>
<tr>
<th>Model</th>
<th>Unstandardized Coefficients B</th>
<th>Std. Error</th>
<th>Standardized Coefficients Beta</th>
<th>t</th>
<th>Sig.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(Constant)</td>
<td>0.313</td>
<td>0.321</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Confidentiality</td>
<td>0.591</td>
<td>0.090</td>
<td>0.578</td>
<td>6.535</td>
</tr>
<tr>
<td></td>
<td>Integrity</td>
<td>0.115</td>
<td>0.088</td>
<td>0.120</td>
<td>1.304</td>
</tr>
<tr>
<td></td>
<td>Availability</td>
<td>-0.116</td>
<td>0.094</td>
<td>-1.20</td>
<td>-1.227</td>
</tr>
<tr>
<td></td>
<td>Verification</td>
<td>8.963E-5</td>
<td>0.097</td>
<td>0.000</td>
<td>0.001</td>
</tr>
<tr>
<td></td>
<td>Privacy</td>
<td>32.8</td>
<td>0.081</td>
<td>0.328</td>
<td>3.990</td>
</tr>
</tbody>
</table>

Based on table 6, it can be observed that the R Square was 0.684, representing that 68.4 percent of the perceived information security can be explained by privacy, integrity, availability, confidentiality and verification. We can conclude the following equation:
Perceived Information Security = β1 Confidentiality + β2 Integrity + β3 Availability + β4 Verification + β5 Privacy + ε

Perceived Information Security = 0.591 * Confidentiality + 0.115 * Integrity – 0.116 * Availability + 0.00000089 Verification + 0.325 Privacy + 0.313

For the individual variables reveals that confidentiality (t-value = 6.535 and p<0.05) and privacy (t-value = 3.990 and p<0.05) were found to have a significant relationship with perceived information security. Therefore, the hypotheses H1 and H5 were supported. Meanwhile integrity (t-value = 1.304 and p>0.05), availability (t-value = -1.227 and p>0.05) and verification (t-value = 0.001 and p>0.05) had no significant relationship with the perceived information security. Hence, H2, H3 and H4 are not supported.

Conclusion and Recommendations:
This study has empirically validated the proposed theoretical framework. All the hypotheses regarding the relationship between the variables are developed and tested using the normality test, reliability test, correlation and multi linear regression. The significant effect influencing the customer perception towards information security in I-system from confidentiality, integrity, availability, verification and privacy are observed. Normality test is being performed as the first test to ensure that the data from the survey instrument is normal. This is because without normality requirement, the result of the analysis will not be accurate. Three type of normality test are being performed namely Shapiro-Wilk, Skewness and Kurtosis test. From the Shapiro-Wilk test, the data collected are normal as the results are above 0.05 for all the variables. The results are further backed by the Skewness and Kurtosis tests as the results for both tests indicated the data are normally distributed. Reliability test on the other hand, is used to ensure all variables in the proposed framework are reliable. It is important for the variables to be reliable as it would impact the analysis of the research and the usage of the results of the research in the future. Using Cronbach’s Alpha Index, all variable are reliable as the results is exceeding 0.7. The exact result for the variables are 0.922 and it is consider as high reliability.

Correlation test also being used to the test the relationship between the variables in the proposed theoretical framework. The reason of correlation test being performed is to investigate whether the issue of multicollinerity is in existence. If multicollinerity exist, it would produce misleading results. From the testing, the correlations of the variables are above 0.5 significant at the 0.01 level (2-tailed). We can conclude that confidentiality variable increases or decreases, integrity variable also increases or decreases as both variables have high correlation with each other. The results show a strong relationship between all the variables. This study employs regression analysis of survey data to measure the customer perception towards information security in I-system system. The results of the regression analysis partially supported the model. Confidentiality and Privacy was found to have significant positive effect on perceived information security. The customers strongly believe personal information is essential to be protected and safeguarded against hackers and criminals. Meanwhile for Integrity, Availability and Verification are not being considered as important variables by the customers. The customers believe that I-system system is an established internet banking systems with advanced tools to secure the internet banking transactions. Therefore, the three variables are not significant. As number of sample for this study is a constraint, there is a possibility that the three variables become significant.

Practical Implications:
The results of this study will have important implications and is believed to be very useful for the Malaysian banking sector and also benefited for the government since both will be aware of the relatively important elements that should be considered to formulate appropriate strategies, promote internet banking service and thus obtaining the benefits from the system. In academic point of view, this study managed to point out some of the significant factors that contributed to the customer’s perception towards information security in internet banking system and specifically to I-system. In addition, this study also provides comparison to other researches on perceived information security in internet banking system. The results of this study will ultimately benefit to bank in knowing how customers perceived I-system system security. Since bank is focusing in getting more usage from I-system, this study help showing the bank management on how important the security in the I-system. Integration between I-system with the legacy system of bank would increase the vulnerability to security risk since the source system is not at par with the modern system for banking institutions. In developing I-system, bank must first ensure high level of security, not just in I-system but include the system that integrates with it. With this research, it will give bank area to focus on in ensuring level of security in I-system.
Additionally, with more oriented steps taken towards the information security, bank has a chance of raising the confidence among the users of I-system in order for them to frequently use the internet banking system. It would indirectly influence other bank customers to experience the convenience of using internet banking as opposed to the traditional banking. Coupled with promotion and advertising on I-system system, it would indeed increase the customer based and would attract new and retained existing customers. With the evolvement in terms of number of usage in internet banking, this will ultimately impact on the bank performance. The profitability may increase due to the high number of customer based using the internet banking system provided by bank. It also give an opportunity for bank to market other products such as loans and credit card to the new and existing customers. By focusing on the real need of the customers, it would hinder bank from spending on unnecessary expenses in order to tackle this important group of people and therefore would increase the profit as lesser expenses are being incurred. bank can be the role model in the banking industry as this will indeed increase the reputation of bank. This would lead to healthy competition between the banks in providing superior internet banking systems to the customers.

This study also benefits to other banks that provide the internet banking services and to others firm that want to introduce the same system application. These related parties must look into the issues and take corrective actions to further increase the security level in their system application. The banking industry will have an example of internet banking system that equipped with controls and the corrective action in case of emergence or malfunctioning of the internet banking system. With a proper internet banking system that addresses customer’s preference in the security area, it will increase the users for such system and depict a good image to the corporation. Furthermore, enhanced security would give impact on the economic of Malaysia as each bank is performing at their maximum in order to cater and grow the internet banking market. From the society point of view, internet banking with superior security would reflect to the usage of the system by customers. With the help of internet banking, people can access any information regarding account and transactions at any time of the day. This means that people no longer have to depend on the office hours of the bank to obtain information. Individual, corporate company and even small medium enterprise are able to fasten their banking transaction thus increase productivity. In addition to this, fund transfers, both national and international, have also become faster and convenient with internet banking. People can easily carry out stock trading, exchanging bonds and other investments with the help of Internet banking. All these features have made Internet banking ideal for people who make a number of financial transactions each day. Furthermore, most people can regularly monitor own account as well as keep track of financial transactions, which can be of immense help in detecting any fraudulent transaction. By using the system, people is expected to used computer as the tools in performing banking transaction and this is in line with the inspiration of the government to turn the country as information technology (IT) country.

This study will also give a rough idea for the government agencies or the regulators in term of monitoring the performance of the banking industry. Nowadays, lots of complaint regarding breaches or lacking of customer personal information that would gain the unauthorized party by exploiting the information have been reported to BNM. This will provide as a platform for BNM to improve and stringent the requirement for internet banking system in order for the safeguarding of the customers personal information. According to our study, confidentiality and privacy is the crucial area that perceived information security by customers. Government can further look into this area and ensure a robust information security policy to the financial institutions. Moreover, with a specific policy pertaining to the identified area would help to build confident to the public in online banking.

Last but not least, for a security system to work well, it’s required a contribution of information from all parties that effected in online transaction i.e. people, corporations and government. From to the literature, future of internet banking in Malaysia is expected that more people will use internet banking while the banks are managing the securities issues and technologies of the service. Moreover, customers may express their concerns and worries while performing the internet banking transaction. From this study they can rest assure that their concerns and worries are reflected to the bank security information system.

**Recommendations for Future Research:**

Although we believe that this study is quite insightful, we still think that it can be further extended to include more respondents from different sectors to make it more realistic and more reliable from the viewpoint of policy makers. Moreover, analysis can be made from people working in different sectors to capture the micro details of internet banking. Further research covering a longer time period with a wider range of internet banking system could reveal some new insights. This study also can be extended to include more internet banking systems from different bank and comparative study between those internet banking providers is one
of the good area of study. A comparative analysis of internet banking security requires further research. Perhaps it might be interesting to study and make a comparison to see whether there exist major differences in different countries. The study may also be extended to cover other fields of perceived information security such as effectiveness, ease of used, prudence and soundness of internet banking and also the magnitude of strength of internal and external variables on internet banking security. In view of the fast rapid internet development in Malaysia, a study of the information security pertaining to any services that require internet access, authentication and security system is worth conducting. Moreover with globalization and internet as the medium of doing business, a study to further analyze the security in the system application globally would be interesting to study.

REFERENCES


Norzaizi, M.D. and Intan Salwani, 2010. Evaluating the intranet acceptance with the extended task-technology fit model: empirical evidence in Malaysian maritime industry”, International Journal of Arts and Science, 3(12): 294-306 and the paper was presented at IJAS Conference, Harvard University, MA, USA.


