INTERNET BANKING SECURITY: HUMAN CENTERED ISSUES IN THE CONTEXT OF THAILAND

Pornchai Ingkathawornwong

Assumption University, Bangkok 10240, Thailand

Corrsponding author: pornchai.i@thaiairways.mail.go.th

Received: March 24, 2019; Revised: November 7, 2019;
Accepted: November 26, 2019

Abstract

This study was motivated by the increasing number of cyber threats to the security of Internet Banking (IB) which is a vital component of banking services in Thailand. The study examined the importance of 75 human-centered issues which were derived from previous studies representing the *customer-side* of IB security in Thailand. Human-centered issues have received relatively little attention in relation to IB security where the focus has been mainly on system-centered concerns and security technologies. The 75 human-centered issues are organized into three categories representing the perspectives of: the bank; the customer; and the attacker. Data was collected by questionnaire from a sample of 91 IB security professionals including 46 working at the operational level of IB and 45 working at the managerial and policy level. The responses from these two groups were analyzed and compared. The 75 human-centered issues examined in the study represent a very satisfactory theoretical framework which could be used in further studies. Practical implications of the findings are identified for those who are involved with IB security as well as others who are concerned with human-centered issues related to the *customer-side* of security regarding finances, transactions, and the confidentiality and privacy of information in the context of IB.

Keywords: E-banking; IB; security; Thailand

Introduction

In order to effectively respond to rapid changes banks and related financial organizations have turned to information technology to improve their productivity and competitiveness. This has encouraged the emergence of new distribution channels that have enhanced the options available for banks to interact with their customers. One of these options is Internet Banking (IB), and even though banks have been providing IB services to customers for many years, security problems still occur and are aggravating.

Solomon (2016) cites Kaspersky Laboratories' comprehensive report on the grim state of online banking security around the world. This leading cyber security solution provider collected the related statistics during the year-long period of 2015. The numbers in the report say it all: 1,966,324 registered notifications of malware raids on online bank accounts; 798,113,087 cyber-attacks launched from online resources worldwide; 2 percent of user-end computers were compromised at least once during the year; around 24 percent of the cyber-attacks originated from United States territory; and 121,262,075 malicious objects (e.g. scripts and exploits) were detected. While social engineering is still very much in use today, more and more vulnerable applications are exploited by tailor-made attacks. These risks involve not only web applications via browsers (62 percent), but also mobile applications due to the rising trend of "*banking on-the-g*o". Around 14 percent of all cyber-attacks on banking targets were executed on the Android mobile platform. Solomon (2016) also notes that the ethical hacker and security expert Sijmen Ruwhof recently exposed the root of the problem in modern banking applications. Hearing about the low security standards of Danish banks Sijmen Ruwhof decided to test the robustness of the website of Danske Bank which is one of the largest in Denmark. The results of his investigation are by no means encouraging.

IB security has to be prioritized to ensure the safety of users and safeguard financial transactions. Commercial banks in Thailand follow the trends by implementing their own IB services. Subsorn and Limwiriyakul (2012) analyzed IB security in Thailand compared to Australia. The results showed that many banks in Thailand try to develop a security fortress in their systems but apply much less effort to security on the *customer-side* even though many reports and studies point to the end user of IB (which is mainly the bank's customers) as the weakest link in IB security. Banks have shown serious interest in security on the *system-side* but IB crime in Thailand still occurs mainly on the *customer-side* which involves human-centered issues as opposed to technical-centered issues which characterize the *system-side* of IB security.

This has motivated this exploratory study which examines the *customer-side* of IB security in Thailand with the aim of improving the reliability and integrity of IB security. The study addresses three related questions:

Question 1: *What are the human-centered issues that are important for examining IB security from the customer-side?*
Question 2: *What is the level of importance of each of the issues in question 1?*
Question 3: *What are the theoretical and practical implications of the findings for questions 1 and 2?*

The study examines and compares the answers to these questions among the members of two groups: an operational group which includes professionals who are mainly responsible for the implementation and continued day-to-day operation of IB security; and a managerial group which includes professionals who are mainly responsible for policy and management concerns for IB security. According to results from many previous studies, IB security has focused mainly on system-centered issues. The internet crime report from ic3 (http://www.ic3.gov) identifies many reports that confirm that in most cases of IB crimes criminals use social engineering techniques that have less concern for system-centered security issues. This research focuses on IB security in relation to human-centered issues by comparing the opinions of two groups who work at either operational level or managerial level positions concerned with IB security. These two groups have different problem interfaces and working perspectives in relation to IB security. Comparing their views about human-centered issues has not been done in previous studies and although this is an exploratory aspect of this study, it is expected to provide findings that benefit both groups and may be influential on both groups in bringing their views into a single focus. It is expected that the findings will contribute to a theoretical understanding of the *customer-*

side of IB security as well as providing practical advice for those concerned with IB security at the operational and managerial levels.

The article is organized as follows. A survey of related literature is presented next followed by a description of the research design and methodology. The results of data analyses are presented followed by a discussion of the findings and final conclusions.

Related Literature and IB Security Issues

Table 1 provides an overview of studies which were influential in the formulation of the *customer-side* IB security issues examined in this study.

Table 1: Overview of Influential Studies

Topic/Focus	Research Approach	Data Collection/ Analysis	Reference
Threats analysis and forecasting on IB and perception of bank's information security concept focus on a Thai commercial bank. Exploring the use of secure socket layer on a Thai bank's website	Qualitative	Descriptive analysis	Subsorn and Limwiriyakul (2012)
Exploring and classifying the vulnerabilities in Online Banking System and Adaptation of security models. The Attack Model and typical scenarios	Case study	Document analysis and literature review	Peotta et al. (2011)
Exploring the technology issues for effective and secure banking transactions and the impact of cost verses profit for banks and the impact of attackers on cost of attacks analysis. IB in India	Explanatory	Literature review	Chakravarti (2015)
Analysis of the Online Banking security issues and evaluation of the security by obscurity policy for Online Banking system. Security analysis on user experiences	Explanatory	Document/Website analysis	Zhang (2012)

Table 1: Continued

Topic/Focus	Research Approach	Data Collection/ Analysis	Reference
The impact of bank's customer personality on IB usage.	Exploratory	Literature review	Yoon and Linsey (2013)
Explore and evaluate on security risks and measures taken for E-Banking solution and example of Online Banking implementation of five-steps approach for access on efforts to protect against external threats. The biggest threats and the weakest link for security	Case study	Case study data	French **(**2012**)**
Bank's perception of adoption of IB and its security and perception of three levels of concentrated security of Online Banking applications in Oman	Qualitative	Surveys	Yousoof and Musaev (2015)
Investigation of five types of risk, security/privacy, financial, social, time; and performance loss	Exploratory	Literature review	Lee (2008)
Exploration of threats on authentication related to passwords. Categorized threats to information security for user privacy/ information	Exploratory	Literature review	Braz and Robert (2006)
Infrastructure security on Web services	Explanatory	Document/website analysis and document review	Claessens (2005)
Reasonable goals for computer system security	Case study	Case study data	Lampson (2004)
Analyses of the effects of diffusion and adopters of mobile banking services (MBS): perceived risk, brand awareness and quantitative brand image of providers, attitude toward using MBS, and study the intention to use MBS in Taiwan.	Explanatory	Questionnaire	Chen (2013**)**

Table 1: Continued

Topic/Focus	Research Approach	Data Collection/ Analysis	Reference
Fintech technology definition and impact on financial service business.	Exploratory	Literature review	Julia (2018)
Total statistic internet crime in USA report, Type of new threats and definition, Statistic and trend of threats compared to earlier years	Exploratory	Literature review	IC3 (2016)
Mobile Banking adoption in South Africa, user perspective and measurement	Exploratory	Literature review	Bankole (2018)
Adoption of IB in Iran from the user perspective.	Exploratory	Literature review	Alizadeh (2018)
Framework measurement of IB system on user perspective	Exploratory	Literature review	Laith (2018)

From Table 1 it is seen that many studies have been exploratory and many were case studies of particular IB providers or customers. Literature reviews have provided very useful summations of research topics and exploratory studies have been common. Among these studies and others, the following discussion highlights several which were especially informative in the selection of important issues to be examined in this study.

Subsorn and Limwiriyakul (2012) stated that IB security issues have become common with harmful impacts on confidentially, integrity, and privacy of the bank and its customers. For the bank’s secured website information they suggest that the IB security should be 128-bit and above the secure socket layer encrypted in order to remove man-in-the-middle external threats. Yoon and Linsey (2013) reported that more than USD 480 million was lost to Internet security crimes in 2011, which represents a 3.4 percent increase since 2010. The target is mainly the bank's customers. Peotta et al. (2011) noted that the number of malware and exploits focused on IB systems vulnerabilities had been steadily growing during past years and that the responsibility for maintaining security is always transferred to the weakest link in the security chain, which means in most cases, the final user. These trends have been reported in many studies in many nations with the emergence of IB.

Peotta et al. (2011) proposed the Attack Tree Model and typical scenarios. The model for common attacks against IB systems is presented in Figure 1. The model includes the main components of banking systems authorization and authentication mechanisms and efficient attacks against them. The attacks exploit vulnerabilities inherent in the people (social engineering and phishing) used to gain control of a device (malware) and credential theft from legitimate users (fake Web pages and malware).

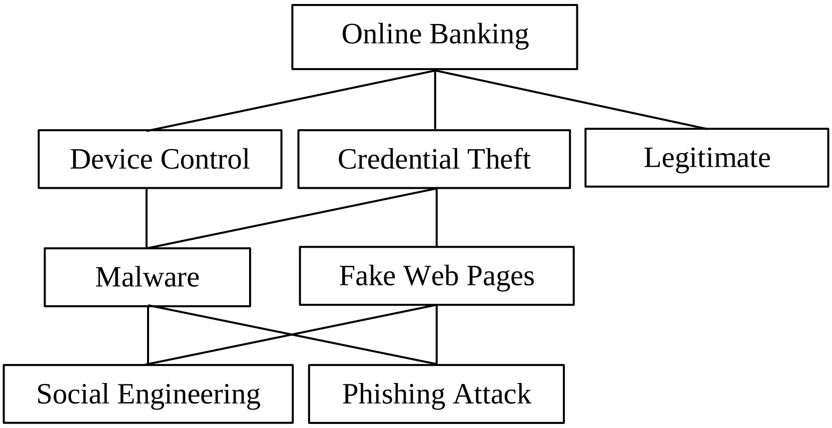

Figure 1: Attack Tree Model (Peotta et al., 2011)

French (2012) noted that all commercial operating systems have vulnerabilities which create opportunities for threats to the information housed on these systems. The threat of user errors can be minimized with validation procedures for data entry and increased training and education for users. The weakest link in IB involves the bank's customers and their knowledge. In relation to Thai banks, Subsorn and Limwiriyakul (2012) observed that some Thai banks were still using very old versions of encryption and digital certification and six out of 12 banks provided wrong secure socket layer encryption information on their websites. They concluded that most of the Thai commercial banks were deficient in providing IB security information to their existing and potential customers.

Alizadeh (2018) has mentioned transaction speed as an important factor for IB. On most websites, sample small images are displayed and users can download them. Most people think that downloading infects the system. This wastes time during the internet exchange and thus users do not have trust in the success of the transactions. Increasing the speed of information processing increases a customer's satisfaction. Increasing trust in the equipment leads to less dissatisfaction and thus it is suggested considering factors that decrease satisfaction may be more important than focusing on factors that increase satisfaction.

According to Julia (2018) the Fintech startup project in 2016 had a large impact on financial services businesses. Fintech adopts automated customer service technologies utilizing chatbots and AI interfaces to assist customers with basic tasks and keep down staffing costs. Fintech is also being leveraged to fight fraud by leveraging information about payment history in order to flag transactions that are outside the norm. Some of the most active areas of fintech innovation include or revolve around the following areas:

Cryptocurrency and *digital cash*; Blockchain technology, including Etherium, a distributed ledger technology (DLT) that maintain records on a network of computers, but has no central ledger; *Smart contracts*, which utilize computer programs (often utilizing the blockchain) to automatically execute contracts between buyers and sellers; *Open banking*, a concept that leans on the blockchain and posits that third-parties should have access to bank data to build applications that create a connected network of financial institutions and third-party providers. An example is the all-in-one money management tool Mint; *Insurtech*, which seeks to use technology to simplify and streamline the insurance industry; *Regtech*, which seeks to help financial service firms meet industry compliance rules, especially those covering Anti-Money Laundering and Know Your Customer protocols which fight fraud; *Robo-advisors*, such as Betterment, utilize algorithms to automate investment advice to lower its cost and increase accessibility; *Unbanked/underbanked*, services that seek to serve disadvantaged or low-income individuals who are ignored or underserved by traditional banks or mainstream financial services companies; and *Cyber-security*, given the proliferation of cybercrime and the decentralized storage of data, cyber-security and Fintech are intertwined.

From many previous studies it is evident that banks try to build IB security on the *system-side* but few of them focus on security threats on the *customer-side* which are associated with human-centered issues of IB security. From previous studies 75 important human-centered issues were identified. These were classified as being related mainly to one of three related perspectives: the Bank Perspective (48 issues); the Customer Perspective (23 issues); or the Attacker Perspective (four issues). This framework of issues, which served as a theoretical basis for the study, is shown as part of Appendix Table A1.

Previous studies address IB security with a main focus on infrastructure system-centered issues. They pay much less attention to the customer-side and especially the human-centered aspects of IB security. This study aims to fill that gap and provide insights specifically related to a wide range of human-centered IB security issues. Furthermore, as part of addressing this gap the separate perspectives of IB staff who work at an operational level and managerial staff working at a management and policy making level are analyzed and compared.

Research Design and Methodology

This exploratory quantitative study aims to develop theoretical and practical knowledge about human-centered IB security issues. The 75 issues, which are derived from a comprehensive review of previous studies, are organized according to the perspective of the bank, the customers, and attackers. The participants are Thai commercial bank officers and IB security staff. In order to provide a broad view of IB security the study examines and compares the views of two groups of participants: those employed at an operational level who are responsible for implementation and day-to-day operation of IB security, and those working at a managerial level who are responsible for management and policy decisions concerning IB security. The sizes of these two populations are unknown and there are no adequate sampling frames available for the random selection of participants. Instead, as in normal practice, a judgmental (or purposive) sampling method was used to select participants. The researcher’s personal contacts were approached first and asked to recommend others suited to the two groups who were then approached individually and asked to participate in the study. Based on the conditions for the validity of the statistical techniques used for data analyses it was decided to target a sample of 50 respondents in each group.

Questionnaire items were designed to measure: **(a)** in Section 1: personal characteristics of participants which were used to develop separate profiles of the operational and managerial groups; and **(b)** in Section 2: the participant's level of agreement with each of the statements associated with the 75 IB security issues. In each case, a 7-point Likert scale ranging from *Strongly Disagree* (**1**) through to *Strongly Agree* (**7**) with *Neutral* (**4**) was used in order to give respondents a scale which allowed for a precise expression of their level of agreement. A notated version of Section 1 of the questionnaire is in Appendix A1 and the 75 items corresponding to the IB security issues are displayed as part of Appendix Table A1.

It is noted that attackers of IB security are not identified or studied as a group in this study. However, the operational and managerial groups are asked to provide their opinions related to the behavior of attackers. It is acknowledged that this is not as good as directly surveying attackers but that was not logistically possible.

Data Analyses

It was possible to collect 46 completed questionnaires from operational level respondents and 45 from managerial level respondents. The 91 returned questionnaires were collected from the initial target of 70 planned questionnaires. The data was entered into an SPSS worksheet and the accuracy of data entry for 10 percent of each group of respondents was checked. No errors were found. The responses were then checked for missing values and none were found and there were no outlier measures among the responses.

The following parts of this section present the results of analyzing the data and form the basis for the discussion of the findings in the following section.

Profile of the Respondents

Responses to Section 1 of the questionnaire were analyzed in order to produce a profile of the respondents in both the operational and managerial groups as shown in Table 2.

Table 2: Profile of the Respondents

Gender	**Operational**			**Managerial**		
	Frequency	Percent		Frequency	Percent	
Male	20	43.5		37	82.2	
Female	26	56.5		8	17.8	
Total	*46*	*100.0*		*45*	*100.0*	
Age (Years)	Frequency	Percent	Cumulative Percent	Frequency	Percent	Cumulative Percent
25 -30	22	47.8	47.8	1	2.2	2.2
31-36	16	34.8	82.6	15	33.3	35.6
37-42	7	15.2	97.8	24	53.3	88.9
43-48	0	0	97.8	3	6.7	95.6
49-54	1	2.2	100.0	2	4.5	100.0
Total	*46*	*100.0*	-	*Total*	*45*	-
Mean (years) = 31.9, Median (years) = 31.0, Mode (years) = 30 and 31, Standard Deviation (years) = 5.2, Skewness = 1.9, Kurtosis = 6.1				Mean (years) = 37.8, Median (years) = 38.0, Mode (years) = 38, Standard Deviation (years) = 4.5, Skewness = 0.9, Kurtosis = 1.4		
Level of Education	Frequency	Percent	Cumulative Percent	Frequency	Percent	Cumulative Percent
Bachelor Degree or Lower	19	41.3	41.3	2	4.4	4.4
Master Degree	25	54.3	95.7	31	68.9	73.3
Doctoral Degree	2	4.3	100.0	12	26.7	100.0
Total	*46*	*100.0*	-	*45*	*100.0*	-
Mean (years) = 17.4, Median (years) = 18.0, Mode (years) = 18, Standard Deviation (years) = 1.4, Skewness = 1.4, Kurtosis = 3.4				Mean (years) = 19.0, Median (years) = 18.0, Mode (years) = 18, Standard Deviation (years) = 1.9, Skewness = 0.9, Kurtosis = 0-.8		

From Table 2, the operational level participants include slightly more females than males. Most are in the age range 25 to 36 years and slightly more than half of them hold a master degree (54 percent) but rarely a doctoral degree (2 percent). For the managerial group, most are males (82 percent) and eighty seven percent are 31to 36 years of age. Most of them hold master degree (69 percent), with 27 percent holding a doctoral degree, and only four percent hold only a bachelor degree or lower. T-tests showed that on average the managerial group is significantly older than the operational group and they have a higher level of formal education ($p < 0.05$). Although there are approximately equal numbers of males and females in the operational group the managerial group is predominantly (82 percent) male. It is concluded that both groups have characteristics which ensure their suitability as subjects for study.

Descriptive Analyses

Appendix Table A1 presents a range of descriptive statistics for each of the variables associated with the 75 IB security issues. In particular, it is seen that the values of skewness and kurtosis are within acceptable limits which satisfy the conditions for the use of the statistics selected for subsequent data analyses (Ott and Hildebrand, 1983). The standard deviations indicate that the responses are consistent with the mean value as a satisfactory representation of the responses. The maximum value for each variable is 7 (*Strongly Agree*) but the minimum value is rarely 1 (*Strongly Disagree*) and instead is often 4 (*Neutral*).

Importance Ratings: If the mean level of agreement with the statement associated with an issue is significantly greater than 5.5 or significantly less than 2.5 ($p < 0.05$) then the issue is regarded as significantly important or significantly unimportant, respectively. Other values for the mean indicate important or unimportant issues if they are greater than or less than the *neutral* value of 4, respectively. For both groups each of the 75 issues had a *level of* importance greater than *neutral*. For the operational group the means range from 4.87 to 6.09 and for the managerial group from 5.49 to 6.49.

T-tests were used to determine the significantly important issues. These are identified in Appendix Table A1 by means notated with *. All of the issues that were rated as being significantly important by the operational group were included among those that were rated as significantly important by the managerial group. T-tests were used to identify issues where there was a significant difference between the means for the groups ($p < 0.05$). In each case where there was a significant difference the mean for the managerial group was significantly greater than the mean for the operational group.

Table 3(a) is derived from Appendix Table A1 and identifies the IB security issues which were considered to be significantly important by the managerial group. Shaded cells in Table 3 identify all of the issues that were considered to significantly important by the operational group. Underlined issues are those where the mean for the managerial group is significantly greater than the mean for the operational group. Table 3(b) complements Table 3(a) and shows the remaining issues which were important but not significantly important for both groups. The four underlined issues in the mean for the managerial group was significantly greater than the mean for the operational group ($p < 0.05$).

Table 3(a): Significantly Important IB Security Issues

IB Security Issue	IB Security Issue
Bank Perspective	Security of transactions
Crimes and security issues that are applicable to IB also apply to almost all other server-client Internet applications.	Confidentiality of personal information
The number of malware and exploits focused on IB systems vulnerabilities has been steadily growing during past years	***Banks should focus on:***
The most widespread IB security threats are those that aim to:	Using the Internet's unique characteristics and capabilities to make their web sites more reliable
Manipulate typical banking customers and their information for illegal gain	Designing IB systems to provide better authentication and identification methods which are less dependent on the user

Table 3(a): Continued

IB Security Issue	IB Security Issue
Focus on infrastructure security	Increasing security of the whole system not just in a single factor/link of the security system
Among the technologies used for IB security:	The use of strong passwords
Technologies used by customers to access IB (e.g. PC, laptop, and mobile) are the weakest link in the security system	Requiring users to regularly change their password
Most of the attacks directed at IB systems:	**Customer Perspective**
Target the user (customer)	***Controlling the risks associated with IB:***
Target the customer's authentication and identification information	Is more important than providing benefits for customers
Use social engineering to obtain customer's authentication and identification information	Inspires high levels of confidence among potential customers
Target the customer's IB access device in order to install malware which automatically performs banking transactions	Inspires high levels of confidence among existing customers
Target the communication channel that links the customer with the bank	***IB providers can develop a customer's trust in IB by:***
For IB systems as:	Providing statements of guarantee
Security is increased there could be a significant negative effect on the usability of the system it's trying to protect	Providing long-term customer service
Despite the proven risk of internal threats:	Providing education/training for customers on security risks
More attention is paid to external threats	***IB customers:***
The following are categories of significant security threats to IB:	Have difficulty in asking for compensation when transaction errors occur
Threats from external sources	***Existing IB customers have significant concerns with:***

Table 3(a): Continued

IB Security Issue	IB Security Issue
Threats from humans	The network security
Threats which are intentional	The reliability of IB web sites
The following are significant consequences of threats to the security of IB:	The security of their banking transactions
Disclosure of information	The privacy of their transactions
Modification of information	Confidentiality of personal information
Destruction of information	***Potential IB customers have significant concerns with:***
Being denied the use of information	The network security
The following are significant threats to IB using reusable passwords:	The reliability of IB web sites
Guessing	The security of their banking transactions
Social engineering	The privacy of their transactions
Eavesdropping	Confidentiality of personal information
Capture and replay	***It is the responsibility of IB providers to:***
Penetration	Determine security policies which set the rules that must be followed for host and network security
Brute force	Offer education programs on security policies and rules for existing and potential IB customers
Point of entry	Educate customers to be able to access their own security weakness and better secure their IB accounts
Revealing secret	**Attacker Perspective**
Significant security threats to IB come from:	***Increased security occurs when attackers believe that:***
The use of a single username and password	The time needed to carry out the attack has increased

Table 3(a): Continued

IB Security Issue	IB Security Issue
For the banking industry the primary concerns for IB are:	The finances needed to carry out the attack have increased
Privacy regarding transactions	The potential punishment for the attack has increased

Table 3(b): Important but Not Significantly Important IB Security Issues

IB Security Issue	IB Security Issue
Bank Perspective	***Significant security threats to IB come from:***
Among the technologies used for IB security:	The fact that an IB environment is less verifiable
Advanced security technology or security methods alone are useless when facing complex attacks targeting customer access technologies (e.g. PC, laptop, and mobile)	The fact that an IB environment is less controllable
The responsibility for:	Anyone with the motivation to gain unauthorized access to the network
Maintaining security is always transferred to the weakest link in the security chain, which in most cases is the customer	Anyone with authorized access to the network
Security incidents can be attributed significantly to poor or unacceptable behavior by customers	**Customer Perspective**
For IB systems as:	***IB providers can develop a customer’s trust in IB by:***
The usability of the systems decreases there is an increase in poor security behaviors by the customers	Increasing familiarity through advertising

Table 3(b): Continued

IB Security Issue	**IB Security Issue**
Despite the proven risk of internal threats:	***IB customers:***
It is widely believed that threats to IB security from bank employees are largely unintentional	Should be more involved in decisions regarding the design of the customer access system used for IB
The following are categories of significant security threats to IB:	***It is the responsibility of IB providers to:***
Threats from internal sources	Develop security awareness programs with universities and government sector organizations
Threats from non-humans	**Attacker Perspective**
Threats which are unintentional	From an attacker’s point of view, security is mainly about what it will cost them to break into the IB environment/system/ platform

Table 4 summarizes the distribution of significantly important issues for each group and the distribution of issues where the importance for the managerial group was significantly greater than for the operational group.

Table 4: Distributions of Significantly Important Items

	Significantly Important Issues		**Distribution within Each Perspective**					
Group	Total Number	Percentage	Bank		Customer		Attacker	
			Number	Percentage	Number	Percentage	Number	Percentage
Managerial	59	79	36	75	20	87	3	75
Operational	16	21	6	13	10	43	0	0
Importance for the Managerial Group Significantly Greater than for the Operational Group								
	41	55	30	63	9	39	2	50

For simplicity, correlations among the 75 variables representing the importance of each issue and the respondents' ages and levels of education are not shown. However: **(a)** For both groups there were numerous significant correlations among the variables representing the issues. This indicated that they are not independent; **(b)** For the operational group: ***(i)*** The only significant correlation with Age was positive and involved the advice that *Banks should focus on increasing security of the whole system not just in a single factor/link of the security system*; ***(ii)*** The only significant correlations with Level of Education were negative and involved three issues: *Crimes and security issues that are applicable to IB also apply to almost all other server-client Internet applications*; *IB customers have difficulty in asking for compensation when transaction errors occur*; and *increased security occurs when attackers believe that the time needed to carry out the attack has increased*; and **(c)** For the managerial group: ***(i)*** The only significant negative correlations with Age involved Level of Education, and two issues: *Significant threats to IB security* are *Threats from non-humans* and *Threats which are intentional*; and ***(ii)*** The only significant positive correlation with Age involved the advice that *it is the responsibility of IB providers to develop security awareness programs with universities and government sector organizations*.

Importance Rankings: Based on the means, the rankings of the 75 issues are displayed in Appendix Table A1. Kendall's tau was used to determine the extent of agreement between the rankings for the operational and managerial groups. The value of Kendall's tau was 0.427 which is statistically significant at a level of 0.01. Consequently, there is significant agreement between the two groups with respect to the rankings of the issues.

The type of rank for an issue is displayed in Appendix Table A1 as high (H), medium (M), or low (L) which indicates that the issues as ranked in position 1-25, 26-50, or 51-75, respectively. Table 5(a) displays issues with the same type of rank for both groups and Table 5(b) shows issues where the type of rank for the groups is different.

Table 5(a): Issues with Same Type of Rank for Both Groups

High Rank	Medium Rank	Low Rank
BANK PERSPECTIVE	**BANK PERSPECTIVE**	**BANK PERSPECTIVE**
Most of the attacks directed at IB systems: Target the customer's authentication and identification information; ***The following are categories of significant security threats to IB:*** Threats from humans; ***For the banking industry the primary concerns for IB are:*** Security of transactions, Confidentiality of personal information; ***Banks should focus on:*** Increasing security of the whole system not just in a single factor/link of the security system, The use of strong passwords. **CUSTOMER PERSPECTIVE** ***Existing IB customers have significant concerns with:*** The security of their banking transactions,	Crimes and security issues that are applicable to IB also apply to almost all other server-client Internet applications; ***Most of the attacks directed at IB systems:*** Target the customer's IB access device in order to install malware which automatically performs banking transactions, Target the communication channel that links the customer with the bank; ***Despite the proven risk of internal threats:*** More attention is paid to external threats; ***The following are significant threats to IB using reusable passwords:*** Point of entry; ***Significant security threats to IB come from:*** The use of a single username and password.	***The responsibility for:*** Maintaining security is always transferred to the weakest link in the security chain, which in most cases is the customer, Security incidents can be attributed significantly to poor or unacceptable behavior by customers; ***For IB systems as:*** The usability of the systems decreases when there is an increase in poor security behaviors by the customers, security is increased there could be a significant negative effect on the usability of the system it's trying to protect; ***Despite the proven risk of internal threats:*** It is widely believed that threats to IB security from bank employees are largely unintentional; ***The following are categories of significant security threats to IB:***

Table 5(a): Continued

High Rank	Medium Rank	Low Rank
Confidentiality of personal information; ***Potential IB customers have significant concerns with:*** The network security, the security of their banking transactions, the privacy of their transactions, Confidentiality of personal information; ***It is the responsibility of IB providers to:*** Determine security policies which set the rules that must be followed for host and network security, educate customers to be able to assess their own security weakness and better secure their IB accounts.	**CUSTOMER PERSPECTIVE** ***Controlling the risks associated with IB:*** Is more important than providing benefits for customers; ***IB providers can develop a customer's trust in IB by:*** Providing education/training for customers on security risks; ***It is the responsibility of IB providers to:*** Offer education programs on security policies and rules for existing and potential IB customers. **ATTACKER PERSPECTIVE** ***Increased security occurs when attackers believe that:*** The finances needed to carry out the attack have increased.	Threats from internal sources, Threats from non-humans, Threats which are unintentional: ***The following are significant threats to IB using reusable passwords:*** Eavesdropping, Brute force, revealing secret; ***Significant security threats to IB come from:*** The fact that an IB environment is less verifiable, the fact that an IB environment is less controllable, anyone with the motivation to gain unauthorized access to the network, and Anyone with authorized access to the network. **CUSTOMER PERSPECTIVE** ***IB providers can develop a customer's trust in IB by:*** Providing statements of guarantee, increasing familiarity through advertising; ***IB customers:*** Should

Table 5(a): Continued

High Rank	Medium Rank	Low Rank
		be more involved in decisions regarding the design of the customer access system used for IB. **ATTACKER PERSPECTIVE** From an attacker's point of view, security is mainly about what it will cost them to break into the IB environment /system/ platform.

Notes: **(a)** Among the 75 issues 43 (57 percent) were ranked in the same manner by the operational and managerial groups.

(b) Among the 43 issues ranked in the same manner by both groups: **(i)** 14 (19 percent) were high rank; **(ii)** 10 (13 percent) were medium rank; **(iii)** 19 (25 percent) were ranked low.

(c) Among these issues with: **(i)** high rank there were 6 (43 percent) issues from the bank perspective, 8 (57 percent) from the customer perspective, and 0 from the attacker perspective; **(ii)** medium rank there were 6 (79 percent) issues from the bank perspective, 3 (30 percent) from the customer perspective, and 1 (10 percent) from the attacker perspective; **(iii)** low rank there were 15 (60 percent) issues from the bank perspective, 3 (33 percent) from the customer perspective, and 1 (7 percent) from the attacker perspective.

Table 5(b): Issues with Different Type of Rank for Each Group

Rank		Managerial Group	
Type		Medium	Low
Operational Group	High	**BANK PERSPECTIVE** ***The following are categories of significant security threats to IB:*** Threats from external sources, Threats which are intentional; ***The following are significant threats to IB using reusable passwords:*** Penetration; ***For the banking industry the primary concerns for IB are:*** Privacy regarding transactions; ***Banks should focus on:*** Using the Internet's unique characteristics and capabilities to make their web sites more reliable. **CUSTOMER PERSPECTIVE** ***Controlling the risks associated with IB:*** Inspires high levels of confidence among potential customers; ***Existing IB customers have significant concerns with:*** The network security, The reliability of IB web sites, The privacy of their transactions. **(13 percent)**	**CUSTOMER PERSPECTIVE** ***Controlling the risks associated with IB:*** Inspires high levels of confidence among existing customers. **(1 percent)**

Table 5(b): Continued

Rank		Managerial Group	
Type		**High**	**Low**
Operational Group	**Medium**	**BANK PERSPECTIVE** The number of malware and exploits focused on IB systems vulnerabilities has been steadily growing during past years; ***Most of the attacks directed at IB system***s: Use social engineering to obtain customer's authentication and identification information; ***The following are significant consequences of threats to the security of IB:*** Disclosure of information; ***The following are significant threats to IB using reusable passwords:*** Social engineering; ***Banks should focus on:*** Designing IB systems to provide better authentication and identification methods which are less dependent on the user, Requiring users to regularly change their password. **CUSTOMER PERSPECTIVE** ***IB providers can develop a customer's trust in IB by:*** Providing long-term customer service; ***IB customers:*** Have difficulty in asking for compensation when transaction errors occur. **(11 percent)**	**BANK PERSPECTIVE** ***Among the technologies used for IB security:*** Advanced security technology or security methods alone are useless when facing complex attacks targeting customer access technologies (e.g. PC, laptop, and mobile); ***The following are significant consequences of threats to the security of IB:*** Modification of information; ***The following are significant threats to IB using reusable passwords:*** Guessing, Capture and replay. **CUSTOMER PERSPECTIVE** ***It is the responsibility of IB providers to:*** Develop security awareness programs with universities and government sector organizations. **ATTACKER PERSPECTIVE** ***Increased security occurs when attackers believe that:*** The time needed to carry out the attack has increased. **(8 percent)**

Table 5(b): Continued

Rank		**Managerial Group**	
Type		**High**	**Low**
Operational Group	**Low**	**BANK PERSPECTIVE** ***The most widespread IB security threats are those that aim to:*** Manipulate typical banking customers and their information for illegal gain; ***Most of the attacks directed at IB systems:*** Target the user (customer). **ATTACKER PERSPECTIVE** ***Increased security occurs when attackers believe that:*** The potential punishment for the attack has increased. **(4 percent)**	**BANK PERSPECTIVE** ***The most widespread IB security threats are those that aim to:*** Focus on infrastructure security; ***Among the technologies used for IB security:*** Technologies used by customers to access IB (e.g. PC, laptop, and mobile) are the weakest link in the security system; ***The following are significant consequences of threats to the security of IB:*** Destruction of information, being denied the use of information. **(5 percent)**

Note: The percentages in each cell indicate the proportion of all of the 75 issues in the cell.

Discussion

The discussion is based on the results of the data analyses presented in the previous section. Findings for each group are discussed first followed by comparisons of the groups, comparisons of the findings with those from previous studies, and finally a discussion of practical implications of the findings.

Managerial Group

The 75 issues examined in this study were important issues in previous studies. From Tables 3(a), (b), and 4 it is seen that their importance is confirmed by the managerial group with none of the issues considered as unimportant and 79 percent considered as significantly important. For this group based on the mean ratings the significantly important issues are focused on the customer perspective with 87 percent of those issues as significantly important while 75 percent of the bank perspective and attacker perspective issues were also considered to be of significant importance. Because a large proportion of the issues are significantly important it is difficult to identify any distinctive patterns across these issues.

However, based on the ranking of the issues shown in Tables 5(a) and (b) it is seen that from the high rank issues that the managerial group's major concerns and advice are as follows:

(a) ***Bank Perspective*****:** The number of malware and exploits focused on IB systems vulnerabilities has been steadily growing during the past years. The most widespread IB security threats are those that aim to manipulate typical banking customers and their information for illegal gain. Most of the attacks on IB systems target customers and use social engineering to obtain a customer's authentication and identification information. For the banking industry the primary concerns for IB are the security and confidentiality of personal information and transactions. Banks should focus on increasing security of the whole system not just in a single part of the security system; the use of strong passwords; requiring users to regularly change their passwords; and the design of IB systems that provide better authentication and identification methods which are less dependent on the user;

(b) ***Customer Perspective*****:** Existing and potential IB customers have significant concerns about asking for compensation when transaction errors occur, the security of their banking transactions, and confidentiality of personal information. Also, potential customers have significant concerns with the security of the network. It is the responsibility of IB providers to determine security policies that must be followed for host and network security and to educate customers to be able to assess their own security weakness and better secure their IB accounts. Providers can develop a customer's trust in IB by ensuring long-term customer service;

(c) ***Attacker Perspective*****:** Increased security occurs when attackers believe that the potential punishment for the attack has increased.

Operational Group

From Tables 3(a), (b), and 4 it is seen that for the managerial group that although none of the 75 issues were considered as unimportant, 21 percent were considered as significantly important. For this group the significantly important issues are focused on the customer perspective with 43 percent of those issues rated significantly important while only 13 percent of the Bank Perspective issues and none of the Attacker Perspective issues were considered to be of significant importance.

As for the managerial group the best indication of the major concerns and advice from the operational group is made evident by considering the issues with a high rank rather than those with a significant mean rating. From Tables 5(a) and (b) these high rank issues concern:

(a) ***Bank Perspective*****:** Most of the attacks directed at IB systems target the customer's authentication and identification information. Significant security threats to IB are intentional and come from external sources. The significant threat to IB using reusable passwords is penetration. For the banking industry the primary concerns for IB are security and privacy of transactions and confidentiality of personal information. Banks should focus on increasing security of the whole system not just in a single part of the system; the use of strong passwords; and using the Internet's unique characteristics and capabilities to make their web sites more reliable:

(b) *Customer Perspective*: Existing and potential IB customers have significant concerns about: network security; the reliability of IB web sites; the privacy and security of their transactions; and the confidentiality of personal information. Controlling the risks associated with IB inspires high levels of confidence among potential and existing customers. It is the responsibility of IB providers to determine security policies that must be followed for host and network security and to educate customers to be able to assess their own security weakness and better secure their IB accounts.

Comparisons between Operational and Managerial Groups

From Tables 3(a), (b), and 4 it is seen that none of the issues were considered as unimportant by either of the groups and all of the issues that were of significant importance to the operational group were also of significant importance to the managerial group. However, for the managerial group 79 percent of the issues were of significant importance compared to only 21 percent for the operational group. For both groups the significantly important issues focused on the issues from the customer perspective followed by the bank perspective and the attacker perspective. Notably, for the operational group none of the attacker perspective issues were significantly important while 75 percent were significantly important for the managerial group. It is possible that compared to the operational group the managerial group may have access to more information about the motivation and behavior of attackers.

From Table 4, 55 percent of the issues were significantly more important to the managerial group than to the operational group. These differences were mainly among bank perspective issues (63 percent) followed by issues for the attacker perspective (50 percent), and the customer perspective (39 percent). The details of these items are presented in Tables 3(a) and (b). The differences reflect the broader experience and understanding of IB security issues and policies among members of the managerial group compared to the more focused practical understandings and experience among the operational group members.

In order to contrast the responses from the two groups it is instructive to compare the ranking of items. The overall rankings by the two groups showed significant agreement (Kendall's tau = 0.427, $p < 0.01$). From Table 5(a) it is seen that overall 57 percent of the issues were ranked in the same manner by the two groups and these were distributed as 25 percent rank to low; 19 percent rank to high, and 13 percent rank to medium.

Issues with a high rank for both groups included 57 percent from the customer perspective and 43 percent from the bank perspective with notably none from the attacker perspective. In summary these issues are:

(a) *Bank Perspective*: Most of the attacks directed at IB target the customer's authentication and identification information. For the banking industry the primary concerns for IB are security of transactions and confidentiality of personal information. Banks should focus on increasing security of the whole system not just in a single part of the security system and the use of strong passwords:

(b) *Customer Perspective*: Existing and potential IB customers have significant concerns with network security, the security of their banking transactions, and the confidentiality and privacy of personal information. It is the responsibility of IB providers to determine security policies which set the rules that must be followed for host and network security and to educate customers to be able to assess their own security weakness and better secure their IB accounts.

At the other extreme, the issues with a low rank by both groups included 60 percent from the bank perspective, 33 percent from the customer perspective, and 7 percent from the attacker perspective. In relation to these low rank issues it is important to note that despite their low rank, none of them was considered to be unimportant by either group. In summary these issues are:

(a) *Bank Perspective*: The responsibility for maintaining security is always transferred to the weakest link in the security chain, which in most cases is the customer and security incidents can be attributed significantly to poor or unacceptable behavior by customers. As the usability of IB systems decreases there is an increase in poor security behaviors by the customers. As security is increased there could be a significant negative effect on the usability of the system it's trying to protect. Despite the proven risk of internal threats, it is widely believed that threats to IB security from bank employees are largely unintentional. Significant security threats to IB include threats from internal sources, from non-humans, and threats which are unintentional. Significant threats to IB using reusable passwords include: eavesdropping, brute force, and revealing secrets. Significant threats come from the fact that an IB environment is less verifiable and controllable, anyone with the motivation to gain unauthorized access to the network, and anyone with authorized access to the network:

(b) *Customer Perspective*: IB providers can develop a customer's trust in IB by providing statements of guarantee and increasing familiarity through advertising. Customers should be more involved in decisions regarding the design of the customer access system used for IB;

(c) *Attacker Perspective*: From an attacker's point of view, security is mainly about what it will cost them to break into the IB environment/system/platform. In particular, among the four issues from the attacker perspective there were two where the groups agreed: *From an attacker's point of view, security is mainly about what it will cost them to break into the IB environment/system/platform* which was low rank for both groups and *Increased security occurs when attackers believe that the finances needed to carry out the attack have increased* which was medium rank for both. With regard to the claim that *Increased security occurs when attackers believe that the time needed to carry out the attack has increased* is medium rank for the operational group and low rank for the managerial group. The two groups are further apart for the remaining issue: *Increased security occurs when attackers believe that the potential punishment for the attack has increased*. This issue has a low rank for the operational group and a high rank for the managerial group. The managerial group clearly places most emphasis on punishment as a deterrent compared to the members of the operational group who emphasize that security will be increased if the time and finances needed to conduct an attack are increased.

From Table 5(b) there are only three other issues for which the groups have opposing positions: two issues from the bank perspective (*The most widespread IB security threats are those that aim to manipulate typical banking customers and their information for illegal gain* and *Most of the attacks directed at IB systems target the user (customer)*). These are low rank for the operational group and high rank for the managerial group. Unlike the managerial group, the operational group does not see the customer as the primary target of security threats. The remaining issue is from the customer perspective (*Controlling the risks associated with IB inspires high levels of confidence among existing customers*) the rank is high for the operational group and low for the managerial group. Although this issue is not unimportant for the managerial group it is not among their high rank issues. This suggests that for them an existing customer's confidence may be positively influenced more by other factors than controlling risks (e.g. better customer service).

Comparisons of the Findings with Previous Studies

A comparison of the findings from this study with those in previous studies is presented in Table 6. Statements related to the issue examined in this study are presented followed by references to previous studies from which the issue was derived. Based on the findings in Table 3(a) and Table 3(b), Table 6 also shows for each group whether or not the statement from the previous studies was supported (S) or not supported (NS).

Table 6: Findings Compared to Previous Studies

Statement of the Issue	References	Operational Level	Managerial Level
The Bank Perspective			
Crimes and security issues that are applicable to Internet Banking also apply to almost all other server-client Internet applications.	Chakravarti, 2015	NS	S
The number of malware and exploits focused on Internet Banking systems vulnerabilities has been steadily growing during past years	Peotta et al., 2011	NS	S
The most widespread Internet Banking security threats are those that aim to:			
Manipulate typical banking customers and their information for illegal gain	Subsorn and Limwiriyakul, 2012	NS	S
Focus on infrastructure security	Claessen, 2005	NS	S
Among the technologies used for Internet Banking security:			
Technologies used by customers to access Internet Banking (e.g. PC, laptop, and mobile) are the weakest link in the security system	Zhang, 2012	NS	S
Advanced security technology or security methods alone are useless when facing complex attacks targeting customer access technologies (e.g. PC, laptop, and mobile)	Zhang, 2012	NS	NS
Most of the attacks directed at Internet Banking systems:			
Target the user (customer)	Peotta et al., 2011	NS	S
Target the customer's authentication and identification information	Peotta et al., 2011	S	S
Use social engineering to obtain customer's authentication and identification information	Peotta et al., 2011	NS	S
Target the customer's Internet Banking access device in order to install malware which automatically performs banking transactions	Peotta et al., 2011	NS	S

Table 6: Continued

Statement of the Issue	References	Operational Level	Managerial Level
Target the communication channel that links the customer with the bank	Lampson, 2004	NS	S
The responsibility for:			
Maintaining security is always transferred to the weakest link in the security chain, which in most cases is the customer	Peotta et al., 2011	NS	NS
Security incidents can be attributed significantly to poor or unacceptable behavior by customers	Lee, 2008	NS	NS
For Internet Banking systems as:			
The usability of the systems decreases when there is an increase in poor security behaviors by the customers	Lee, 2008	NS	NS
When security is increased there could be a significant negative effect on the usability of the system it's trying to protect	Braz and Robert, 2006;	NS	S
Despite the proven risk of internal threats:			
It is widely believed that threats to Internet Banking security from bank employees are largely unintentional	Keller and Powell, 2005	NS	NS
More attention is paid to external threats	Dinnie, 1999	NS	S
The following are categories of significant security threats to Internet Banking:			
Threats from internal sources	Loch and Warkentin, 1992;	NS	NS
Threats from external sources	Loch and Warkentin, 1992;	S	S
Threats from humans	Loch and Warkentin, 1992;	NS	S
Threats from non-humans	Loch and Warkentin, 1992;	NS	NS

Table 6: Continued

Statement of the Issue	References	Operational Level	Managerial Level
Threats which are intentional	Loch and Warkentin, 1992;	S	S
Threats which are unintentional	Loch and Warkentin, 1992;	NS	NS
The following are significant consequences of threats to the security of Internet Banking:			
Disclosure of information	Lee, 2008	NS	S
Modification of information	Lee, 2008	NS	S
Destruction of information	Lee, 2008	NS	S
Being denied the use of information	Lee, 2008	NS	S
The following are significant threats to Internet Banking using reusable passwords:			
Guessing	Fegghi and Williams 1999	NS	S
Social engineering	Fegghi and Williams 1999	NS	S
Eavesdropping	Fegghi and Williams 1999	NS	S
Capture and replay	Fegghi and Williams 1999	NS	S
Penetration	Fegghi and Williams 1999	NS	S
Brute force	Fegghi and Williams 1999	NS	S
Point of entry	Fegghi and Williams 1999	NS	S
Revealing secret	Fegghi and Williams 1999	NS	S
Significant security threats to Internet Banking come from:			
The fact that an Internet Banking environment is less verifiable	Yoon and Linsey, 2013	NS	NS
The fact that an Internet Banking environment is less controllable	Yoon and Linsey, 2013	NS	NS
The use of a single username and password	Lee, 2008	NS	S
Anyone with the motivation to gain unauthorized access to the network	Chen, 2013	NS	NS
Anyone with authorized access to the network	Chen, 2013	NS	NS

Table 6: Continued

Statement of the Issue	References	Operational Level	Managerial Level
For the banking industry the primary concerns for Internet Banking are:			
Privacy regarding transactions	Subsorn and Limwiriyakul, 2012; Chakravarti, 2015	NS	S
Security of transactions	Subsorn and Limwiriyakul, 2012; Chakravarti, 2015	S	S
Confidentiality of personal information	Subsorn and Limwiriyakul, 2012; Chakravarti, 2015	S	S
Banks should focus on:			
Using the Internet's unique characteristics and capabilities to make their web sites more reliable	French, 2012	S	S
Designing Internet Banking systems to provide better authentication and identification methods which are less dependent on the user	Peotta et al., 2011	NS	S
Increasing security of the whole system not just in a single factor/link of the security system	Claessen, 2005	S	S
The use of strong passwords	Lee, 2008	NS	S
Requiring users to regularly change their password	Lee, 2008	NS	S
The Customer Perspective			
Controlling the risks associated with Internet Banking:			
Is more important than providing benefits for customers	Yoon and Linsey, 2013	NS	S
Inspires high levels of confidence among potential customers	Yoon and Linsey, 2013	NS	S
Inspires high levels of confidence among existing customers	Yoon and Linsey, 2013	NS	S

Table 6: Continued

Statement of the Issue	References	Operational Level	Managerial Level
Internet Banking providers can develop a customer's trust in Internet Banking by:			
Providing statements of guarantee	Yoon and Linsey, 2013	NS	S
Increasing familiarity through advertising	Yoon and Linsey, 2013	NS	NS
Providing long-term customer service	Yoon and Linsey, 2013	NS	S
Providing education/training for customers on security risks		NS	S
Internet Banking customers:			
Have difficulty in asking for compensation when transaction errors occur	Yoon and Linsey, 2013	NS	S
Should be more involved in decisions regarding the design of the customer access system used for Internet banking	French, 2012	NS	NS
Existing Internet Banking customers have significant concerns with:			
The network security	French, 2012	S	S
The reliability of Internet Banking web sites	Furnell, 2004	S	S
The security of their banking transactions	Subsorn and Limwiriyakul, 2012; French, 2012; Chakravarti, 2015	S	S
The privacy of their transactions	Furnell, 2004; Subsorn and Limwiriyakul , 2012; French, 2012; Chakravarti, 2015	NS	S
Confidentiality of personal information	Subsorn, 2011; French, 2012; Chakravarti, 2015	NS	S
Potential Internet Banking customers have significant concerns with:			
The network security	French, 2012	S	S
The reliability of Internet Banking web sites	Furnell, 2004	S	S

Table 6: Continued

Statement of the Issue	References	Operational Level	Managerial Level
The security of their banking transactions	Subsorn and Limwiriyakul, 2012; French, 2012; Chakravarti, 2015	S	S
The privacy of their transactions	Furnell, 2004; Subsorn and Limwiriyakul, 2012; French, 2012; Chakravarti, 2015	S	S
Confidentiality of personal information	Subsorn and Limwiriyakul, 2012; French, 2012; Chakravarti, 2015	S	S
It is the responsibility of Internet Banking providers to:			
Determine security policies which set the rules that must be followed for host and network security	French, 2012	S	S
Offer education programs on security policies and rules for existing and potential Internet Banking customers	French, 2012	NS	S
Educate customers to be able to access their own security weakness and better secure their Internet Banking accounts	Lee, 2008; Subsorn and Limwiriyakul, 2012	S	S
Develop security awareness programs with universities and government sector organizations	Subsorn and Limwiriyakul, 2012	NS	NS
The Attacker Perspective			
From an attacker’s point of view, security is mainly about what it will cost them to break into the Internet Banking environment/system/ platform	Lampson, 2004; Chakravarti, 2015	NS	NS
Increased security occurs when attackers believe that:			
The time needed to carry out the attack has increased	Zhang, 2012; Chakravarti, 2015	NS	S

Table 6: Continued

Statement of the Issue	References	Operational Level	Managerial Level
The finances needed to carry out the attack have increased	Zhang, 2012; Chakravarti, 2015	NS	S
The potential punishment for the attack has increased	Zhang, 2012; Chakravarti, 2015	NS	S

As seen from Table 4 there were noticeable differences between the operational and managerial level groups regarding the level of support they showed for the statements derived from previous studies displayed in Table 6. For the managerial level group there was considerable support for statements from previous studies: 75 percent for issues classified as representing the bank and attacker perspectives; and 87 percent support for statements representing the customer perspective. For the operational level group, the level of support was much less: 43 percent support for statements representing the customer perspective; only 13 percent support for statements representing the bank perspective; and no support for statements representing the attacker perspective.

Practical Implications

The findings have identified and compared important issues identified by operational and managerial groups working at different levels in relation to IB security. From the findings there are issues where both groups agree (e.g. Table 5(a) and shaded issues in Table 3(a)) and others where they disagree (e.g. Table 5(b) and underlined issues in Tables 3(a) and (b)). It is expected that these findings are of practical interest to both groups and that they provide insights for each group into the thinking of the other group. This is expected to lead to better understandings between the groups which will inform and benefit the collegial development of IB security with respect to policies, management, and implementation.

Among the findings there are selected important issues which have direct implications for practice:

(a) Most of the attacks directed at IB systems ***(i)*** manipulate typical banking customers and their information for illegal gain; ***(ii)*** are intentional and from external sources; and ***(iii)*** use malware and social engineering to target the customer's authentication and identification information;
(b) For banks and existing and potential customers the primary concerns for IB are security of transactions, confidentiality and privacy of transactions and personal information;
(c) Banks should focus on ***(i)*** increasing security of the whole system, not just a single part of the security system; ***(ii)*** the use of strong passwords; ***(iii)*** security policies which set the rules that must be followed for host and network security; ***(iv)*** educating customers to be able to assess their own security weakness and better secure their IB accounts; ***(v)*** using the Internet's unique characteristics and capabilities to make their web sites more reliable; ***(vi)*** controlling risks associated with IB; ***(vii)*** designing IB systems to provide better authentication and identification methods less dependent on the user; ***(viii)*** requiring users to regularly change their password; ***(ix)*** providing long-term customer service; ***(x)*** making it easy for customers to request compensation when transaction errors occur; and ***(xi)*** advocating for increased punishment for IB security attacks.

Conclusion

In relation to the three research questions for the study presented in the Introduction section:
Question 1: *What are the human-centered issues that are important for examining IB security from the customer-side?* Seventy-five human-centered issues were derived from a comprehensive review of previous studies representing the *customer-side* of IB security. These issues were organized according to three perspectives (bank, customer, and attacker) which enhanced the analyses and presentation of the findings;
Question 2: *What is the level of importance of each of the issues in question 1?* The full details of the findings are presented in the preceding Discussion section. In summary: **(a)** For both groups none of the issues were unimportant; **(b)** 79 percent of issues were significantly important for the managerial group compared to only 21 percent for the operational group. For both groups they were focused on the customer perspective. For the operational group none of the

issues from the attacker perspective were significantly important; **(c)** The managerial group rated 55 percent of the issues to be significantly more important than the operational group and these issues were mainly from the bank perspective; **(d)** There was significant agreement between the two groups for the overall ranking of the issues with 57 percent of the issues ranked in the same manner by both groups. Most agreement was among low rank issues followed by those with high rank; **(e)** For the operational group most of the high rank issues were from the customer perspective with none from the attacker perspective. For the Managerial group most were from the Bank Perspective followed by the customer perspective and then the attacker perspective.

The differences between the groups reflected the Managerial group's more extensive policy and management level experience with IB security. Compared to the operational group those in the managerial group have access to more information about IB security issues as they affect their organizations.

Question 3: *What are the theoretical and practical implications of the findings for questions 1 and 2?* The 75 human-centered issues categorized in three perspectives served as a useful theoretical framework for the study of the *customer-side* of IB security. Practical implications of the findings are presented in the preceding Discussion section where are number of actions to be taken by banks is described. The findings have practical importance for both managerial and operational IB security professionals as well as others associated with online security concerned with financial transactions, confidentiality, and privacy of organizational and personal information.

There are limitations on the findings. The study is exploratory in nature and the external validity of the findings can only be enhanced by repetition of the study. In particular, it would be desirable to have larger samples of operational and managerial professionals. It was not possible to include a group of attackers (hackers) for this study. However, this limitation may be addressed in further studies if a group of such individuals would participate. Also, it may be useful to include a separate group of experienced IB users (customers) in future studies even though in this study it is reasonable to assume that the managerial and operational group members were also experienced IB users.

References

Alizadeh, A. (2018) *Effects of Adoption and satisfaction on word of mouth in the Internet Banking of Iran*. [Online URL: www.icommercecentral.com/open-access/effects-of-adoption-and-satisfaction-on-word-of-mouth-in-the-internet-banking-of-iran.php?aid=87221] accessed on October 12, 2018.

Bankole, F. O. (2018) *Influences on Cell Phone Banking Adoption in South Africa: An Updated Perspective*. [Online URL: www.icommercecentral.com/open-access/influences-on-cell-phone-banking-adoption-in-south-africa-an-updated-perspective.php?aid=86260#corr] accessed on October 12, 2018.

Braz, C. and Robert, J. (2006) Security and Usability: The Case of the User Authentication Methods. *Proceedings 18th International Conference of the Association Francophone d'Interaction Homme-Machine*, Montreal, Quebec, 199-203.

Chakravarti, P. K. (2015) An Analysis of security issues in E-Banking. *International Journal of Management, Information Technology and Engineering* 3(8): 1-8.

Chen, C. S. (2013) Perceived risk, usage frequency of mobile banking services. *Managing Service Quality: An International Journal* 23(5): 410-436.

Claessens, J. (2005) Web services and web services security standards, Nova Dubley-Gough. *Information Security Technical Report* 10(1): 15-24.

Dinnie, G. (1999) The Second Annual Global Information Security Survey. *Information Management and Computer Security* 7(3): 125-128.

Fegghi, J. and Williams, P. (1999) *Digital Certificates: Applied Internet Security*. Massachusetts: Addison Wesley Longman Inc.

French, A. M. (2012) A case study on E-banking security - When security becomes too sophisticated for the user to access their information. *Journal of Internet Banking and Commerce* 17(2): 1-14.

Furnell, S. (2004) E-commerce security: A question of trust. *Computer Fraud and Security* 10(1): 10-14.

IC3 (2016) Internet Crime Complaint Center: Annual Report. [Online URL: pdf.ic3.gov/2016_IC3Report.pdf] accessed on October 12, 2018.

Julia, K. (2018) *Breaking down Fintech*. [Online URL: www.investopedia.com/terms/f/fintech.asp] accessed on October 12, 2018.

Keller, S. and Powell, A. (2005) Information Security Threats and Practices in Small Business. *Information Systems Management* 22(2): 7-19.

Laith, T. K. (2018) *Framework for Measuring the Convenience of Advanced Technology on User Perceptions of Internet Banking Systems*. [Online URL: www.icommercecentral.com/open-access/framework-for-measuring-the-convenience-of-advanced-technology-on-user-perceptions-of-internet-banking-systems.php?aid=86276] accessed on October 12, 2018.

Lampson, B. (2004) Computer Security in the Real World. *IEEE Computer* 37(6): 37-46.

Lee, M. C. (2008) Factors influencing the adoption of Internet Banking: An integration of TAM and TPB with perceived risk and perceived benefit. *Electronic Commerce Research and Applications* 8(1): 130-141.

Loch, K. and Warkentin, M. (1992) Threats to Information Systems: Today's Reality, Yesterday's Understanding. *MIS Quarterly* 17(2): 173-186.

Ott, L. and Hildebrand, D.K. (1983) *Statistical Thinking for Managers*. Boston: Duxbury.

Peotta, L. et al. (2011) A Formal Classification of Internet Banking Attacks and Vulnerabilities. *IJCSIT* 3(1): 186-197.

Solomon, S. (2016) *All You Wanted to Know About Online Banking Security Checkmarx*. [Online URL: www. checkmarx.com/2016/01/17/wanted-know-online-banking-security/] accessed on May 25, 2016.

Subsorn, P. and Limwiriyakul, S. (2012) A Comparative Analysis of Internet Banking Security in Thailand: A Customer Perspective. *Procedia Engineering* 32(1): 260-272.

Yoon, H. S. and Linsey, M. (2013) Development of a quantitative model of the impact of customer' personality and perceptions on Internet Banking use. *Computers in Human Behavior* 29(1): 1133-1141.

Yousoof, M. and Musaev, E. (2015) A Review on Internet Banking Security and Privacy Issues in Oman, ICIT 2015. *The 7th International Conference on Information Technology*. [Online URL: www.researchgate.net/publication/277954759] accessed on May 25, 2016.

Zhang, F. (2012) *An Analysis of the Online Banking Security Issues Reported* by Hole, Moen, and Tjostheim. [Online URL: www.cs.auckland.ac.nz/courses/compsci725s2c/archive/termpapers/fzhang.pdf] accessed on May 15, 2016.

Appendix

A1. Notated Questionnaire

Section 1: Personal Information

1. Age **(AGE)**: … years **2.** Gender **(GENDER)**: □ Male **(1)** □ Female **(2)**

3. Highest level of education **(EDU)**: □ Bachelor degree or lower **(16)** □ Master degree **(18)** □ Doctoral degree **(22)** **4.** Number of months of experience in your current work position **(EXP)**: … months **5.** The main level of your involvement with security issues **(LEVEL)**: □ ***Operational level***, which means that you work mainly at an operational level as a professional responsible for the implementation and continued day-to-day operation of security systems related to IB **(1)** □ ***Managerial level***, which means that you work mainly as a professional responsible for issues related to policy and management concerns for security systems related to IB **(2)**

Table A1: Descriptive Statistics for Responses to Section 2 of the Questionnaire

		Operational						**Managerial**					
Variable	**IB Security Issue**	Mean	Standard Deviation	Skewness	Kurtosis	Rank	Rank Type	Mean	Standard Deviation	Skewness	Kurtosis	Rank	Rank Type
	Bank Perspective												
BP1	Crimes and security issues that are applicable to IB also apply to almost all other server-client Internet applications.	5.57	1.03	-.31	-1.01	37.5	M	6.02*	.94	-1.41	2.20	46	M
BP2	The number of malware and exploits focused on IB systems vulnerabilities has been steadily growing during past years	5.70	1.03	-.24	-1.05	28.5	M	6.44*	.81	-1.53	1.99	3.5	H
The most widespread IB security threats are those that aim to:													
BP3	Manipulate typical banking customers and their information for illegal gain	5.37	.97	-.37	-.53	58	L	6.20*	.91	-1.15	.72	22.5	H
BP4	Focus on infrastructure security	5.22	1.26	-1.47	2.61	65	L	6.11*	1.07	-1.85	3.74	33	M

Table A1: Continued

Variable	**IB Security Issue**	**Operational**						**Managerial**					
		Mean	Standard Deviation	Skewness	Kurtosis	Rank	Rank Type	Mean	Standard Deviation	Skewness	Kurtosis	Rank	Rank Type
Among the technologies used for IB security:													
BP5	Technologies used by customers to access IB (e.g. PC, laptop, and mobile) are the weakest link in the security system	5.02	1.60	-.69	-.53	72.5	L	6.07*	1.05	-1.84	3.40	42	M
BP6	Advanced security technology or security methods alone are useless when facing complex attacks targeting customer access technologies (e.g. PC, laptop, and mobile)	5.52	1.28	-1.02	.42	44	M	5.51	1.68	-1.22	.21	73.5	L
Most of the attacks directed at IB systems:													
BP7	Target the user (customer)	5.41	1.31	-.83	.45	55.5	L	6.20*	1.07	-1.21	.16	22.5	H

Table A1: Continued

		Operational						Managerial					
Variable	**IB Security Issue**	Mean	Standard Deviation	Skewness	Kurtosis	Rank	Rank Type	Mean	Standard Deviation	Skewness	Kurtosis	Rank	Rank Type
BP8	Target the customer's authentication and identification information	5.85*	1.01	-.76	.20	17	H	6.24*	.77	-1.07	1.43	17.5	H
BP9	Use social engineering to obtain customer's authentication and identification information	5.70	.96	-.90	1.16	28.5	M	6.38*	.88	-1.25	.57	8	H
BP10	Target the customer's IB access device in order to install malware which automatically performs banking transactions	5.54	1.22	-1.47	2.69	40.5	M	6.11*	.64	-.10	-.52	33	M
BP11	Target the communication channel that links the customer with the bank	5.70	.94	-.68	.42	28.5	M	6.07*	1.23	-1.35	.82	42	M
The responsibility for:													
BP12	Maintaining security is always transferred to the weakest link in the security chain, which in most cases is the customer	5.13	1.52	-1.23	1.70	67.5	L	5.69	1.24	-1.46	2.14	70	L

Table A1: Continued

Variable	IB Security Issue	Operational						Managerial					
		Mean	Standard Deviation	Skewness	Kurtosis	Rank	Rank Type	Mean	Standard Deviation	Skewness	Kurtosis	Rank	Rank Type
BP13	Security incidents can be attributed significantly to poor or unacceptable behavior by customers	5.43	1.22	-.53	-.09	52	L	5.76	1.33	-1.33	1.28	66	L
For IB systems as:													
BP14	The usability of the systems decreases there is an increase in poor security behaviors by the customers	5.02	1.37	-.47	-.35	72.5	L	5.87	1.34	-1.16	.51	60	L
BP15	Security is increased there could be a significant negative effect on the usability of the system it's trying to protect	5.07	1.25	-.62	-.02	70.5	L	5.93*	1.11	-1.19	.79	55	L
Despite the proven risk of internal threats:													
BP16	It is widely believed that threats to IB security from bank employees are largely unintentional	5.07	1.47	-1.09	.54	70.5	L	5.60	1.28	-1.74	1.49	72	L

Table A1: Continued

Variable	**IB Security Issue**	**Operational**						**Managerial**					
		Mean	Standard Deviation	Skewness	Kurtosis	Rank	Rank Type	Mean	Standard Deviation	Skewness	Kurtosis	Rank	Rank Type
BP17	More attention is paid to external threats	5.57	1.07	-1.20	1.90	37.5	M	6.13*	.96	-1.38	1.94	29	M
The following are categories of significant security threats to IB:													
BP18	Threats from internal sources	5.20	1.39	-1.19	.90	66	L	5.76	1.35	-1.26	1.08	66	L
BP19	Threats from external sources	5.80*	.98	-1.06	1.44	19.5	H	6.09*	.76	-1.11	2.01	38	M
BP20	Threats from humans	5.74	1.08	-.76	.14	24.5	H	6.36*	.77	-1.34	2.06	10.5	H
BP21	Threats from non-humans	5.43	1.38	-1.27	1.56	52	L	5.93	1.45	-1.51	1.29	55	L
BP22	Threats which are intentional	5.89*	.99	-.76	.32	14	H	6.11*	.77	-1.72	2.73	33	M
BP23	Threats which are unintentional	5.13	1.42	-1.15	1.69	67.5	L	5.84	1.27	-1.26	1.04	62.5	L
The following are significant consequences of threats to the security of IB:													
BP24	Disclosure of information	5.52	1.15	-.42	.35	44	M	6.27*	.80	-.80	-.14	16	H
BP25	Modification of information	5.61	.93	.18	-.93	34.5	M	5.96*	1.20	-1.94	3.21	53	L
BP26	Destruction of information	5.41	1.11	-.28	.58	55.5	L	6.04*	1.26	-1.37	1.42	44.5	M

Table A1: Continued

Variable	IB Security Issue	Operational						Managerial					
		Mean	Standard Deviation	Skewness	Kurtosis	Rank	Rank Type	Mean	Standard Deviation	Skewness	Kurtosis	Rank	Rank Type
BP27	Being denied the use of information	4.89	1.39	-.16	.17	74	L	6.09*	.87	-.81	.19	38	M
The following are significant threats to IB using reusable passwords:													
BP28	Guessing	5.50	1.24	-.54	-.61	47	M	5.84*	1.14	-1.13	2.74	62.5	L
BP29	Social engineering	5.61	.93	-.33	.14	34.5	M	6.20*	1.01	-.97	-.30	22.5	H
BP30	Eavesdropping	5.39	1.06	.06	-1.21	57.0	L	5.98*	.86	-.83	.44	51	L
BP31	Capture and replay	5.61	1.04	-.11	-1.13	34.5	M	5.87*	1.19	-.64	-.83	60	L
BP32	Penetration	5.78	.96	-.62	.28	21	H	6.13*	.75	-.88	1.22	29	M
BP33	Brute force	5.33	1.30	-1.02	.96	60.5	L	5.98*	.89	-.55	-.35	51	L
BP34	Point of entry	5.72	.98	-.42	-.07	26	M	6.09*	.79	-1.02	1.42	38	M
BP35	Revealing secret	5.43	1.17	-.58	-.31	52	L	5.89*	.91	-.71	-.02	57.5	L
Significant security threats to IB come from:													
BP36	The fact that an IB environment is less verifiable	5.11	1.29	-.53	-.02	69	L	5.76	1.36	-1.59	2.10	66	L

Table A1: Continued

Variable	IB Security Issue	Operational						Managerial					
		Mean	Standard Deviation	Skewness	Kurtosis	Rank	Rank Type	Mean	Standard Deviation	Skewness	Kurtosis	Rank	Rank Type
BP37	The fact that an IB environment is less controllable	5.28	1.36	-.70	-.17	63	L	5.69	1.18	-1.68	2.04	70	L
BP38	The use of a single username and password	5.54	1.21	-1.18	1.79	40.5	M	6.09*	1.22	-1.21	2.37	38	M
BP39	Anyone with the motivation to gain unauthorized access to the network	5.35	1.178	.04	-1.23	59	L	5.49	.99	-.99	.90	75	L
BP40	Anyone with authorized access to the network	5.43	1.13	-.75	-.07	52	L	5.51	1.35	-.96	.01	73.5	L
For the banking industry the primary concerns for IB are:													
BP41	Privacy regarding transactions	5.76	1.04	-.74	.48	22.5	H	6.18*	.98	-1.42	1.91	26.5	M
BP42	Security of transactions	5.93*	1.06	-.79	-.04	11.5	H	6.44*	.72	-1.67	2.81	3.5	H
BP43	Confidentiality of personal information	5.87*	1.02	-.63	-.07	16	H	6.38*	.80	-1.08	.34	8	H
Banks should focus on:													

Table A1: Continued

Variable	**IB Security Issue**	**Operational**						**Managerial**					
		Mean	Standard Deviation	Skewness	Kurtosis	Rank	Rank Type	Mean	Standard Deviation	Skewness	Kurtosis	Rank	Rank Type
BP44	Using the Internet's unique characteristics and capabilities to make their web sites more reliable	6.00*	.97	-.92	.81	7.5	H	6.18*	.86	-1.70	3.20	26.5	M
BP45	Designing IB systems to provide better authentication and identification methods which are less dependent on the user	5.46	1.41	-1.27	1.89	49	M	6.29*	.89	-1.60	3.07	14.5	H
BP46	Increasing security of the whole system not just in a single factor/link of the security system	5.89*	.97	-1.29	4.14	14	H	6.49*	.54	-.38	-1.00	1	H
BP47	The use of strong passwords	5.74	1.24	-1.02	.87	24.5	H	6.31*	.79	-.91	.17	12.5	H
BP48	Requiring users to regularly change their password	5.54	1.260	-1.21	1.41	40.5	M	6.20*	.75	-1.01	1.52	22.5	H
						Customer Perspective							
Controlling the risks associated with IB:													

Table A1: Continued

Variable	**IB Security Issue**	**Operational**						**Managerial**					
		Mean	Standard Deviation	Skewness	Kurtosis	Rank	Rank Type	Mean	Standard Deviation	Skewness	Kurtosis	Rank	Rank Type
CP1	Is more important than providing benefits for customers	5.70	1.05	-.42	-.46	28.5	M	6.00*	.90	-1.35	2.38	48	M
CP2	Inspires high levels of confidence among potential customers	5.76	.99	-1.19	3.24	22.5	H	6.11*	.93	-1.45	2.45	33	M
CP3	Inspires high levels of confidence among existing customers	5.89	.85	-.24	-.67	14	H	5.93*	.78	-1.68	3.74	55	L
IB providers can develop a customer's trust in IB by:													
CP4	Providing statements of guarantee	5.33	1.25	-.73	.57	60.5	L	5.87*	1.16	-1.55	2.64	60	L
CP5	Increasing familiarity through advertising	5.30	1.36	-.58	.47	62	L	5.73	1.25	-.99	.01	68	L
CP6	Providing long-term customer service	5.67	1.03	-.42	-.91	31	M	6.20*	.99	-1.00	-.09	22.5	H
CP7	Providing education/training for customers on security risks	5.50	1.23	-.37	-1.05	47	M	6.07*	.83	-1.10	1.32	42	M

Table A1: Continued

Variable	IB Security Issue	Operational						Managerial					
		Mean	Standard Deviation	Skewness	Kurtosis	Rank	Rank Type	Mean	Standard Deviation	Skewness	Kurtosis	Rank	Rank Type
IB customers:													
CP8	Have difficulty in asking for compensation when transaction errors occur	5.54	1.03	.00	-1.10	40.5	M	6.20*	1.07	-1.55	2.06	22.5	H
CP9	Should be more involved in decisions regarding the design of the customer access system used for IB	4.87	1.41	-.40	.32	75	L	5.78	1.12	-1.33	2.13	64	L
Existing IB customers have significant concerns with:													
CP10	The network security	6.07*	.90	-.69	-.25	4.5	H	6.00*	1.06	-1.41	1.66	48	M
CP11	The reliability of IB web sites	6.09*	.87	-.38	-1.02	2	H	6.00*	.95	-1.15	1.44	48	M
CP12	The security of their banking transactions	6.09*	.93	-.54	-.84	2	H	6.29*	1.05	-1.58	1.75	14.5	H
CP13	The privacy of their transactions	5.80	1.11	-.31	-1.29	19.5	H	6.13*	1.10	-1.77	3.72	29	M
CP14	Confidentiality of personal information	5.83	1.25	-.79	.13	18	H	6.24*	.95	-1.33	1.76	17.5	H

Table A1: Continued

Variable	**IB Security Issue**	**Operational**						**Managerial**					
		Mean	Standard Deviation	Skewness	Kurtosis	Rank	Rank Type	Mean	Standard Deviation	Skewness	Kurtosis	Rank	Rank Type
Potential IB customers have significant concerns with:													
CP15	The network security	6.00*	1.25	-1.72	4.32	7.5	H	6.22*	.92	-1.44	3.26	19	H
CP16	The reliability of IB web sites	6.00*	.97	-.46	-.93	7.5	H	6.04*	.92	-1.16	1.71	44.5	M
CP17	The security of their banking transactions	6.09*	1.15	-1.18	3.35	2	H	6.44*	.72	-1.29	1.67	3.5	H
CP18	The privacy of their transactions	5.96*	1.12	-1.02	3.42	10	H	6.44*	.81	-1.27	.64	3.5	H
CP19	Confidentiality of personal information	6.00*	1.05	-.71	-.70	7.5	H	6.42*	.86	-1.83	3.25	6	H
It is the responsibility of IB providers to:													
CP20	Determine security policies which set the rules that must be followed for host and network security	6.07*	.93	-.65	-.48	4.5	H	6.38*	.53	.05	-1.03	8	H
CP21	Offer education programs on security policies and rules for existing and potential IB customers	5.61	1.26	-.61	-.24	34.5	M	6.11*	.93	-1.15	3.73	33	M

Table A1: Continued

		Operational						Managerial					
Variable	**IB Security Issue**	Mean	Standard Deviation	Skewness	Kurtosis	Rank	Rank Type	Mean	Standard Deviation	Skewness	Kurtosis	Rank	Rank Type
CP22	Educate customers to be able to assess their own security weakness and better secure their IB accounts	5.93*	.98	-.61	-.53	11.5	H	6.31	.79	-1.20	1.45	12.5	H
CP23	Develop security awareness programs with universities and government sector organizations	5.65	1.10	-.30	-1.20	32	M	5.69	.99	-.33	-.86	70	L
	Attacker Perspective												
AP1	From an attacker's point of view, security is mainly about what it will cost them to break into the IB environment/system/ platform	5.43	1.15	-1.21	3.52	52	L	5.89	1.30	-1.40	1.80	57.5	L
Increased security occurs when attackers believe that:													
AP2	The time needed to carry out the attack has increased	5.52	1.11	-.05	-1.32	44	M	5.98*	1.13	-1.60	2.93	51	L

Table A1: Continued

Variable	IB Security Issue	Operational						Managerial					
		Mean	Standard Deviation	Skewness	Kurtosis	Rank	Rank Type	Mean	Standard Deviation	Skewness	Kurtosis	Rank	Rank Type
AP3	The finances needed to carry out the attack have increased	5.50	1.09	-.26	-.84	47	M	6.09*	1.04	-1.83	3.61	38	M
AP4	The potential punishment for the attack has increased	5.26	1.56	-1.05	.87	64	L	6.36*	1.04	-1.64	1.92	10.5	H

Notes: **(a)** * for the mean indicates that the mean is significantly greater than 5.5 (p < 0.05); **(b)** Rankings are from 1 (*Most Important*) to 75 (*Least Important*); **(c)** Rank types high (H), medium (M), and low (L) correspond to rank positions 1-25, 26-50, and 51-75, respectively.