Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2008 Proceedings

Americas Conference on Information Systems (AMCIS)

2008

Securing Personal Information Assets: Testing Antecedents of Behavioral Intentions

Jongki Kim
Pusan National University, jkkim1@pusan.ac.kr

Kirk P. Arnett
Mississippi State University, kpal1@msstate.edu

Gary F. Templeton
Mississippi State University, gtempleton@cobilan.msstate.edu

Securing Personal Information Assets: Testing Antecedents of Behavioral Intentions

Jongki Kim
Pusan National University, So. Korea
Jkkim1@pusan.ac.kr

Kirk P. Arnett
Mississippi State University
Kpa1@msstate.edu

Gary F. Templeton
Mississippi State University
gtempleton@cobilan.msstate.edu

ABSTRACT

Due to the increased global reliance on information technology, and the prominence of information resources value, identity theft is a problem domain effecting millions of computer users annually. The realities of identity theft are highly visible in the global media, although empirical investigations on the topic are limited. The purpose of this study is to identify and analyze perceptions of personal information (e.g., identity) as it relates to perceived threats, mitigation, perceived risks, and intended safe information practice intentions. We propose a risk analysis model based on theoretical variables that have been researched and extensively used in both government and private sector organizations. The model is empirically tested using LISREL to perform structural equation modeling. Findings indicate support for a relationship between risk and both 1) behavioral intentions to perform safe information practices and 2) personal information asset value.

KEYWORDS

Security, Risk, Identity Theft, Behavioral Intentions

INTRODUCTION

Between corporate and personal information (PI) assets, we live in a world of insecurity. It is clear that both information systems and the information they contain are vulnerable and risks to these systems and information will continue. Risks to information systems and PI have dramatically increased as society becomes more immersed in the information age. Both traditional information systems and the newer social oriented systems share more information with and about more people than ever before. Each week we see a new and perhaps heretofore unknown story in the popular literature regarding threats, risks, and vulnerabilities to information stored or transmitted by hardware, software, and network systems created by a variety of vendors – no single system or single vendor is immune to threats.

The information assets go beyond PI that is usually stored and processed by corporate information systems and extends to that which is stored by individuals. Identity theft, which has imposed expensive and time consuming hardships on its victims, is an ongoing global concern[1]. In the US, the *Identity Theft and Assumption Deterrence Act of 1998* made PI theft with the intent to commit an unlawful act a federal crime. The Act designates the Federal Trade Commission to serve as an advocate for victims of identity fraud (Saunders, 1999).

For PI, the realities of identity theft are strongly visible in popular press and in news media. Unfortunately, the scholarly investigation of this problem domain is limited. The purpose of this paper is to identify and analyze how individuals assess their PI as an asset along with the associated vulnerabilities and perceived threats and risks. Given such an assessment, what intentions do individuals have regarding safeguard controls? This assessment is accomplished here by a survey of perceptions and intentions of business students who are presumed to be heavy computer users because of their college requirements, and whose identity is easily exposed to those who could or

[1] The FTC is active in the identity theft education arena as a search of their web site at http://ftc.org yields more than 7,000 "identity theft" matches. They have published information showing that the identity theft problem is growing.

would misuse it. We administered a survey to 176 US college of business students for analysis of risk assessment model fit.

The significance of this study is observable in a large number of recent stories appearing in a wide range of media including popular press and TV, academic study, and professional analysts' research. Studies done by both Gartner Research and Harris Interactive (2003) indicated that in the previous 12 months, approximately seven million people had been victims of identity theft involving fraud charges averaging more than $90,000 each. Despite these findings, Neumann (2008) brings an overall conclusion from a body of literature over the past that "risky problems are as great today as they were when we first set out to expose and eradicate them" (p. 80). He further believes that a huge challenge to our community is to bridge the gap between theory and practice.

"It is safe to infer now, more than ever, that individuals are at a high risk of having their personal identifiable information compromised and then used by criminals" (Okenyi and Owens, 2007, p. 310). While PI security has been the responsibility of information systems managers, the issue should be of major significance to corporate managers: "Infosecurity is no longer an ivory tower issue…It is now a key function that is critical in protecting the bottom line" (Grant, 2007, p. 48). This impact is shared by Elms, LaPrade and Maurer (2008): "The companies that learn how to reduce the frequency and/or severity of the different hacking risks will be rewarded with an increase in firm value as compared to their competitors" (p. 4).

This paper examines the perceptions and intentions of future business professionals with an eye toward IP security awareness. It contributes to existing knowledge regarding risk analysis, perceptions and intentions by examining an established organizational British model (CRAMM) for information security risk analysis as the model parameters relate to the individual intention for safe information practices. The practices of individuals remain confusing as they are aware of risks to personal information assets through widespread media attention, yet they continue to engage in practices that reason dictates are illogical. As an example, this year's famous 6th annual social engineering experiment by Gibbs (2008) revealed that 21% of the 576 people questioned gave away sensitive information for a chocolate bar. It is the findings regarding individual safe practice intentions that contribute to the stream of risk analysis study.

Toward that end, the remainder of this paper is organized into four major sections. The first section describes the background of **Protecting Personal Information (PI**) from a corporate and individuals view. The **Model Development** follows and includes the proposed model and hypotheses. The **Methodology** follows the model and hypotheses, and a discussion of the **Results** of the LISREL tests provides the final section of this research.

BACKGROUND: PROTECTING PERSONAL INFORMATION

According to the Federal Trade Commission (FTC) collection of citizen complaints, credit card fraud (26%) was the most common form of reported identity theft followed by phone or utilities fraud (18%), bank fraud (17%), and employment fraud (12%) (FTC, 2005). Other significant categories of identity theft reported by victims were government document or benefits fraud (9%) and loan fraud (5%). The average time spent by victims in restoration is about 300 hours and this may take years to accomplish. Three forms of identity theft were described. Financial identity theft, which involves the imposter's use of personal identifying information, primarily the Social Security number, to establish new credit lines in the name of the victim is the first. Criminal identity theft occurs when a criminal gives another person's personal identifying information in place of his or her own to law enforcement. Identity cloning is the third category in which the imposter uses the victim's information to establish a new life. The perpetrator lives and works as the victim. The discussion that follows includes organizational level responsibility for the protection of personal information, then individual-level responsibility, and concludes with personal information risk management.

Personal Information and Organizational-Level Responsibility

The risk exposure of individuals during Internet shopping extends to the organizations, which are the dominant online sellers. A recent study by Wang and Head (2007) found that risk perception plays an important role in e-commerce trust building which leads to a high level of relationship intention among the participants. But the risks certainly extend beyond ecommerce buying and selling. Now even seemingly harmless browsing can lead to personal identity compromise. The continuation of phishing and pharming attacks is a testament to the value that PI holds for individuals who do not own that information.

Organizations have a responsibility to maintain watch over the PI that they maintain for customers, employees, and suppliers. Today it is rare to view a corporate website that does not have some written statement regarding care and protection of personal identity information. This is in sharp contrast to the situation just over ten years ago when Liu, Marchewka, Lu and Yu (2005) reported only 52% of the Fortune 500 contained a privacy policy link from their home pages. Today, US citizens have been strongly urged to take precautions against the menace of ID theft. But what have we done, should we do, and can we do? Regardless of the answers, we must acknowledge that a part of the PI protection responsibility lies with us, but alas, much of the protection of our PI is in the hands of others where we have little or no control. Risk management is the key to protection whether via individuals or business.

Exposed personal computers exist in both homes and businesses. As individuals we recognize the risks associated with computer infections and we may fight to protect PI on our PCs with multiple technical safeguards such as firewalls, antivirus and anti-spyware software (which also dominate corporate protection controls as determined in the 2007 CSI survey). Also as an individual, we might simply want to become better informed about various threats and exercise or at least intend to exercise better and safer practices when using online computer access. Presently, most organizations do not have the necessary safeguards in place to protect individual identification information. Table 1 lists the most serious corporate security breaches of 2006. Still, it is not only organizations that must be held accountable. While organizations are losing PI through server attacks, software compromise, and laptop thefts, individuals are losing PI from their home computers and mobile devices.

Organization	Event	# of Records
Boeing	Stolen laptop with employee records	382,000
Aetna	Backup tapes stolen from a strategic alliance	130,000
UCLA	Database of student & Faculty Information Hacked	800,000
Starbucks	Loss of multiple laptops with employee data	60,000
Colorado Dept of Human Services	Stolen desktop with customer and staff data	1,400,000
Akron Children's Hospital	Breach of database with patient data	253,900
General Electric	Stolen laptop with employee records	50,000
Circuit City	Chase credit services misplaced tape with credit card holder data	2,100,000
Department of Transportation	Stolen laptop with driver's license holder information	132,400
Kaiser	Stolen laptop with customer data	160,000

Table 1: Significant Data Breaches of 2006 (source: Hines, 2007)

Personal Information and Individual-Level Responsibility

Internet shopping has been considered high-risk individual-level behavior for the past decade. A Forrester Research study reported that almost two-thirds of respondents reported not buying products online due to concerns about the security of their PI (Portz, Strong, Busta, and Schneider, 2000), and some argue that the concerns are worsening as the public becomes more aware of the information risks involved in Internet shopping (Perez, 2005). For an individual, the risk associated with PI loss depends on the value the individual places on the types of information.

Social security numbers (SSN) have more value than other types of PI. The SSN has been labeled as the 'Holy Grail' of information (Berghel, 2000) because with it, data aggregation is easily accomplished and all other PI becomes more readily available. This asset should have enormous value to its true owner and more than small value to those non-owners who would steal and misuse it. Berghel (2007) points out the historical usage creep of the SSN as a personal identifier and the dangers surrounding that use. Once, as Berghel put it, "the toothpaste was out of the tube" and the use of the SSN had spread beyond its intended use for the Social Security Administration, it quickly became a unique personal identifier, not only for the government, but also for educational institutions and organizations outside of the government. There are currently multiple efforts to contain the spread of the SSN, but these efforts have proven to be too little and too late.

Given that the online threats are increasing and ever-changing, one can question how individuals are trying to protect their PI. After an evaluation of perceived threats, risks, and asset value, computer users theoretically have a range of potential response behaviors. Perhaps the most influential theory that is used for intentions is Ajzen's (1991) Theory of Planned Behavior. This theory describes behavioral intentions and behavior as a product of attitudes toward the behavior, perceived subjective norm, and perceptions of the problems related to the behavior (Ajzen, 1991). For online users, the attitude captures an overall evaluation of engaging in risk prevention strategies. This can be measured by perceived usefulness and value. The subjective norm refers to a person's perception of how important others perceive the behavior. The perceived behavioral control refers to the user's controllability over resources and protection of private information as well as the skills of conducting the behavior (Pavlou and Fygenson, 2006).

The individual-level responsibility to protect PI is a motivator of this study. We wish to illuminate the relationship between the perceived PI threats and risks of individual users and their mitigation responses. The possible response behaviors by individuals, who have fewer resources to devote to controls, also extend to the responsibilities of organizations to protect PI.

Personal Information Risk Management

The intent of risk management is to quantify the impact of exercised threats. Identification of risks and the costs involved in their mitigation surround the risk management process. Risk management can be, and often is, accompanied by financial justifications. An authoritative CSI survey indicates that 77% of organizations responding to the *12th CSI Computer Crime and Security Survey* acknowledge conducting some form of economic evaluation of their security expenditures using quantitative measures of ROI (39%), IRR (21%) or NPV (17%) (Richardson, 2007). The study suggests that despite the criticality of protection, managers believe that justification of security expenditures is needed for senior management approval. The significance of using capital budgeting techniques for evaluating information security assets often depends on the "support of senior level management" (Okenyi and Owens, 2007, p. 307).

If cost justification, as noted by CSI (2007) and Okenyi and Owens (2007), is extended to the individual level of analysis, each person who perceives threats to PI (assets) must make a judgment as to the worth of each mitigation strategy. That is, one might ask, is it worth $29.95 each year to reduce the risks of spyware to my home computer? In this sense, the individual is performing a cost-benefit analysis regarding risk management. The point of this discussion is that the individual, much like the corporation, uses risk analysis in his or her risk management practices. Kosba (2008) also drives this point as he states: "current privacy theory regards people's privacy related behavior as the result of a situation-specific cost-benefit analysis, in which the potential risk of disclosing one's personal information are weighed against potential benefits of disclosure"(p. 25). The extent of use of a specific mitigation strategy is a function of individual perceptions of asset value, threats, and mitigation response costs. But, mitigation strategies may well differ when dealing with digitized personal information.

How individuals take and respond to risks comes from different biological, psychological, and social causes. Yet there is confusion in the different ways that individuals deal with personal risks and personal information risks related to computers. In the former case people often think through risks and deliberately assume them. In contrast, when dealing with computers, people seem to take risks "unconsciously and in some cases unwillingly." (Zegans, 2008, p. 152.) This supports arguing for additional education and training to increase awareness.

MODEL DEVELOPMENT

Vulnerabilities and threats to an individual's PI asset change over time. Therefore, individuals cannot make a single decision with regard to safe information practices. Rather, users continually evaluate the components of asset value, mitigation strategies, threats and risks to form intentions as to courses of action. "Risk mitigation involves the process of prioritizing, evaluating, and implementing appropriate controls" (Dhillon, 2007, p. 166). Three essential components of risk management are risk assessment, risk mitigation, and risk evaluation. Risk assessment includes the identification and evaluation of risks so as to assess the potential impact and results in safeguard controls. In order to determine the likelihood of future adverse events the "threats, vulnerabilities and controls must be evaluated together" (Dhillon, 2007, p. 158). The interplay between the three dictates the impact that an adverse event might have. Similarly the government's NIST 800-30 (http://csrc.**nist**.gov/publications/**nist**pubs/800-30/sp800-30.pdf) risk determination helps assess the level of risks. The level of risk is a function of the likelihood of a threat exploiting vulnerability, the magnitude of the impact of the threat, and the adequacy of existing or planned controls. These relationships are also implemented in the British government's *CCTA Risk Analysis and Method Management (CRAMM)* (Siemens, 2007) model, and Yim's (2002) risk assessment model.

Proposed Model

ASSET, THREAT, MITIGATION STRATEGY, RISK, and BEHAVIORAL INTENTION are the building blocks of the research model shown as Figure 1. It extends risk analysis baseline theory of CRAMM by including user intention to secure assets as the dependent variable in the management of PI risk.

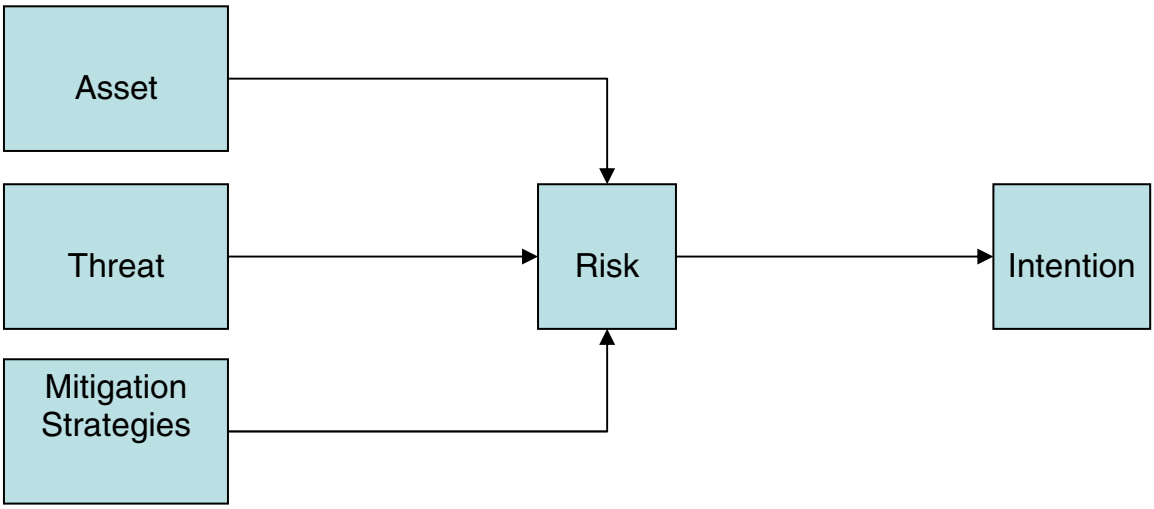

Figure 1: A Personal Identity Risk Research Model

The model identifies the interplay suggested by Dhillon (2007) and noted in NIST 800-30, Yim (2002), and the British CRAMM models. For the present study, each of the model components may be explained as they apply to individual PI. The ASSET is the PI of the individual. As noted earlier, individuals place different values on their PI and further some components of PI, such as SSN, may be ascribed more value than others such as cellular telephone number. The THREATS to PI are exemplified by hackers, virus code, phishing attacks, etc. MITIGATION is the exercise of and extent of control being used to safeguard against the threat. This interplay provides for the RISK as shown in the CRAMM study model. The final component of the model is INTENTIONS. These are measured by variables that ask what the user plans to do with regard to technical features and safe practices.

It is our contention, as in the models that have been briefly reviewed, that PI risks like organizational risks are dependent on asset values (called systems characteristics in 800-30), threats, and vulnerabilities. Risk is often a surrogate measure of how much security we do or do not have. It is operationalized here as the probability that a threat will exploit a weakness of a system. A threat is any environmental contingency or event with the potential to cause harm. Thus, risk is a function of environmental threats and successful organizations respond to threats using

risk management methods. Although the interest in this research is toward individuals, a corporate perspective as relayed in the models is appropriate as individual risks may come from carelessness of an organization or individual. Regardless of source, damage to PI is at least one result.

Hypothesis Development

The preceding discussion has indicated a tie between organizations and individuals with regard to risk analysis, especially when this analysis uses PI as the asset of concern. This discussion leads us to propose four hypotheses for the preliminary model suggested in Figure 1.

It is widely accepted that IS managers assign higher risk levels based on how they prioritize the assets they protect. As explained by Ortega (2007), the link between asset and risk valuation is caused by the tendency of attackers to target higher-valued information assets: "High-value corporate assets are becoming more marketable on black markets, making cybercrime extremely profitable. The asset-risk valuation association is well articulated by Macaulay (2006), who describes assets as having varying degrees of "risk conducting" (p. 13) properties. As noted, risk management includes asset identification and evaluation. For these reasons, we hypothesize that as the asset value increases, so does perception of risk:

Hypothesis 1: As the asset value increases, so does perception of risk.

As individuals perceive greater threats to their information assets, they should perceive greater risks to PI. As incidents of attacks continue to rise, so will the need for risk management (Thomas, 2004). This logic is used in Yim's (2002) risk model. Because perceptions of threats influence perceived risk, economic changes occur in the field of information security (Grant, 2007, p. 48). Neglecting risks while threats increase has been documented as a major cause of security breach: "The underlying problem is that many managers are not well versed on the nature of systems risk, likely leading to inadequately protected systems" (Straub and Welke, 1998, p. 442). Therefore, we hypothesize a relationship between perceived threats and perceived risks:

Hypothesis 2: As the perceived threat increases, so does the perception of risk.

Perceived risk is also influenced by mitigation strategies employed to combat security breaches. This relationship is expected for at least two reasons. First, the malware landscape changes rapidly and the attackers always seem to be one step ahead of the defenders. Mitigation strategies may lead to risk because "risks are increasing faster than the amelioration of those risks" (Neumann, 2003, p. 136). In high reliability situations, small errors can lead to severe outcomes and consequences so that risk mitigation is critical to survival on the organization (Grabowski & Roberts, 1998). Similarly, important elements of PI such as a SSN or credit card number need not be compromised multiple times as one compromise can lead to extensive damage. Further, multiple risk exposure is not required for compromise as one exposure can result in severe loss. In these situations mitigation is critical for the reduction of risks. An alternate view is that mitigation strategies work against the goal of risk reduction because they may cause an over-reliance on systems and an under-reliance on people. Thus, people could rely heavily on formal countermeasures and become less aware of threats and risks. We take the first, more conventional, and more logical view regarding risks associated with personal information.

Hypothesis 3: As mitigation strategies increase, perceived risk is reduced

As users perceive the risk of security breaches to increase, they are likely to change their behavioral intentions pertaining to security defense. The theory of reasoned action (TRA) suggests that perceived risk or anxiety influences behavioral intentions (Liu et al, 1997), an important motivator of actual behavior (Venkatesh, Morris, Davis, and Davis, 2003). Ajzen's (1991) theory of planned behavior suggests that intentions are related to attitude and to a perception of problems. For online users, the attitude captures an overall evaluation of encountering risks. For these reasons, we hypothesize a relationship between perceived risk and the behavioral intentions to reduce risks:

Hypothesis 4: As perceived risk increases, so does behavioral intention to reduce risks

METHODOLOGY

This study involves creation of a model to be used for individual risk analysis related to the protection of the personal information asset or personal identity information. This protection is essential in today's world where compromises of PI have become an epidemic. To test the model a survey was administered and the survey data was used to test the four hypotheses developed in support of the research model.

Survey

The survey instrument shown in Appendix A is based on several established standards. In part the questions mirror some of the questions used to examine perceptions of computer viruses in the mid 1990's (Jones, et al.) The study found that college students, at that time had reasonably strong knowledge concerning the threats of computer viruses, which had been infecting computers for several years when the questionnaire was administered. Later this survey was expanded to capture knowledge concerning spyware (Schmidt & Arnett, 2005). Also included are questions from a study of security concerns in Ecommerce by Chen, Schmidt, Phan, and Arnett (2008).

Sa*mple*

From the survey administration in the college of business, 176 questionnaires were collected. Among them, 19 were excluded due to missing values. Therefore, 157 responses were used in the data analysis. The sample is dominated by male respondents (66.1%) which is not typical of the university or college enrollment, but likely mirrors the fact that the respondents for this study were enrolled in an MIS or information security course. This heavy male enrollment is typical of MIS enrollments at this institution. The respondents in total are young with 96% of them being under 30 years of age and, as expected, all of them have at least some college education. Moreover, more than one-half of these respondents report that they spend eleven or more hours per week using the Internet. The large categorical percentages indicate need for change to the initial instrument before expansion of this study to other subjects and countries.

RESULTS

Data analysis was conducted with the two-step approach suggested by Anderson and Gerbing (1988). LISREL 8.51 was used in the analysis. The first step was to conduct instrument validation beginning with unidimensionality analysis (Garver and Mentzer, 1999). As suggested by Gefen, Karahanna, and Straub (2003) items which had a high degree of residual variance with other items were deleted one by one. This process resulted in deleting several items such as TH4, RM1, RSK1, RSK5, RSK6, and INT4. The correlation matrix is available as Appendix 2.

Composite construct reliability (CCR) and average variance extracted (AVE) are commonly used to assess construct reliability. Fornell and Lacrker (1981) suggested a threshold value of 0.7 for CCR and 0.5 for AVE. All coefficients exceeded those values as shown in Table 2 below. Therefore construct reliability is evident.

Construct validity is usually assessed in terms of two aspects; convergent validity and discriminant validity (Gefen, 2003). Commonly used criteria for convergent validity are for a standardized loading of greater than 0.5 and a t-value that is greater than 2.0 (Bagozzi and Yi, 1988). All indicators were larger than 0.5 and each indicator significantly loaded on the corresponding construct and construct validity is verified.

Construct	Item	Loading	t-value	S.E.	CCR	AVE
Asset	AS1	.93	15.40	.13	.951	.762
	AS2	.89	14.05	.22		
	AS3	.89	14.20	.21		
	AS4	.92	14.93	.16		
	AS5	.83	12.64	.31		
Threat	TH1	.80	11.58	.37	.884	.656
	TH2	.84	12.50	.30		
	TH3	.84	12.66	.29		
	TH5	.76	1.87	.42		
Mitigation	RM2	.62	8.46	.61	.894	.683
	RM3	.80	11.79	.37		
	RM4	.93	15.02	.14		
	RM5	.92	14.79	.15		
Risk	RSK2	.88	13.90	.22	.936	.830
	RSK3	.93	15.00	.14		
	RSK4	.92	14.93	.15		
Intention	INT1	.84	12.64	.29	.900	.636
	INT2	.88	13.63	.22		
	INT3	.82	12.13	.33		
	INT5	.78	11.38	.39		

Table 2: Item Loadings and Construct Reliabilities

Discriminant validity is the extent to which an item measures a uniquely defined latent construct (Gefen, 2003). There are several methods to examine discriminant validity. This study employed a method suggested by Fornell and Lacrker (1981) in which the square root of AVE of a construct is compared with the corresponding correlation coefficients. If the square root value is greater than any of corresponding row and column of correlation coefficients, then construct validity is held. As shown in Table 3 below, constructs in this study satisfied the above criteria.

	AVE	ASSET	THREAT	MITGATION	RISK	INTENTION
ASSET	.762	**.873***				
THREAT	.656	.727	**.810**			
MITIGATION	.683	.508	.568	**.826**		
RISK	.830	.580	.508	.412	**.911**	
INTENTION	.636	.678	.599	.522	.464	**.797**

*diagonals are square root of AVE

Table 3: Discriminant Validity

Table 4 below shows the overall model fit statistics for the research model. Some of the indices are less than satisfactory. This is due to the insignificant relationships shown in the research model from Figure 1. Among the four paths of the model, only those from 'Asset' to 'Risk' and from 'Risk' to 'Intention' are significant at the .01 level. Thus while some of the hypotheses can be validated, the model as a whole does not fit. This absence of fit is between mitigation and risk and threat and risk.

Goodness of Fit Indices	Research Model	Desired Level*
X^2	421.18	Smaller
Df	163	-
X^2/df	2.58	<3.0
GFI	.79	>.90
AGFI	.73	>.80
Standardized RMR	.15	<.05
RMSEA	.097	.05-.08
NFI	.97	>.90
CFI	.97	>.90

*desired levels are from Teo et al. (2003)

Table 4: Overall Model Fit

The model and its significance are shown as Figure 2. Although via CRAMM three factors were supposed to influence the level of risk perceived by users, only the 'Asset' factor proved to be significant. The significant relationship between 'Asset' and 'Risk' implies that as the value of the asset (any PI needing protection from identity theft) increases, individuals assume a heightened risk perception associated with stolen identity. On the other hand, users do not perceive (or perhaps understand) that risks are threats that can be exercised, and that mitigation controls may aid in risk reduction, but not completely eliminate risks.

CONCLUSIONS

In terms of paths in the proposed model, two were significant at the 0.01 level: asset value to risk, and risk to intention. These are positive points, but not necessarily intuitive. Increased personal asset value, whether monetary or perceived, will result in greater perceived risks to the individual owner of the asset. More importantly, as the risk increases, then individuals will intend to better protect their information assets. Two other paths of the experimental model were not significant. While the model fit can be described as marginally successful, the lack of fit between mitigation and risk leaves questions. The central one is whether or not mitigation really does influence risk perception in either direction.

A possible explanation for the absence of fit between mitigation strategies and risk is that users do not foresee that current mitigation strategies will continue to eliminate risk. This finding has an important implication for security managers, who presumably expect safeguard controls to reduce risk – this expectation may never be met. This finding shows that mitigation does not equate to the elimination of risks. Such false expectations for mitigation strategies have generated insignificant relationships between these two constructs in our setting. For example, if I assume that once installed, and anti-spyware application will protect me against all spyware, then I will be disappointed. If I do not continue the mitigation strategy and continually update the software, then new spyware, which was unavailable at the time of the original installation of the software, will become a risk. This is particular true in the malware battleground where even the best known anti-virus companies are foiled by hackers, and these companies too have been the targets of successful attacks.

As for the absence of fit in the model between threat and risk, the close association between the two may be another source of confusion in the perceptions of the respondents. For example, a threat can be defined as "a circumstance or event with the potential to cause harm" (Krutz and Vines, p. 936) and a risk as "the likelihood that a threat will occur" (Krutz and Vines, p. 929), then this causal relationship may be perceived as being the same by a non-security conscious expert. It is possible that, even though the connection is theoretical, the difference in organizational commitment and individual commitment to manage risks is dissimilar because legislation may dictate corporate policy and practice. Individuals have no such external motivations.

Our results indicate that individual perceptions of risks and the intentions for security mitigation depend on three factors: 1) the value that the individual places on his PI assets, 2) the severity of the threats against that asset, and 3) the extent of mitigation practices in place. For instance, fear appeals (LaRose et al, 2005) such as those frequently shown on TV regarding identity theft, will result in different responses for different users. These responses are a function of how much the person who views the appeals believes him or herself to be vulnerable to the threat, and the extent of damage that an exercised threat would generate. For corporate America, the responses to threats may be dictated with legislation. For example, the *Personal Data Privacy & Security Act of 2007* which was initially presented to the Senate as follows:

> *"To prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information."*

This kind of legislation should reduce the list of threats noted in Table 1 so that risk can be mitigated. Furthermore, an 'awareness prescription' has been proposed in recent published work by Okenyi and Owens (2007): "The best control against this attack is education by training people to be aware of the value of the information assets at their disposal as well create awareness of human hacking techniques, which makes it easy for them to diagnose a social engineer" (p. 306). Further, before PI risk management can be successful, management needs to understand the significance of ongoing awareness: "In order to secure the support of senior level management, it is necessary to help them understand that security awareness is a vital element in protecting the organization information assets" (Okenyi and Owens, 2007, p. 307).The present study has several limitations. We have not attempted to measure understanding, and have rather stood by testing a specific model's parameters. It is likely that knowing a risk and understanding a risk would produce different responses, especially in terms of mitigation strategies. This study used all levels of undergraduate students as subjects. While students have well known limitations as subjects, this is not believed to be a serious concern in this study because these students should be as aware of information theft as the normal population. More importantly, these students were enrolled in an MIS course, and as such they may be more aware of information security concerns because of the subject matter. In that regard there may be a limitation of students who do not mirror the general population of students as these could be using mitigation strategies as a part of class assignments. Of lesser concern are the geographic limits of the study as it was confined to one university in the US. But information theft, while presently a larger threat in the US, is expected to grow rapidly once ecommerce payment systems and similar mechanisms that expose digital secrets become more popular. The questions answered in this study must be answered in larger context both in the US and in other countries as well and they need to be answered with a more diverse group of students.

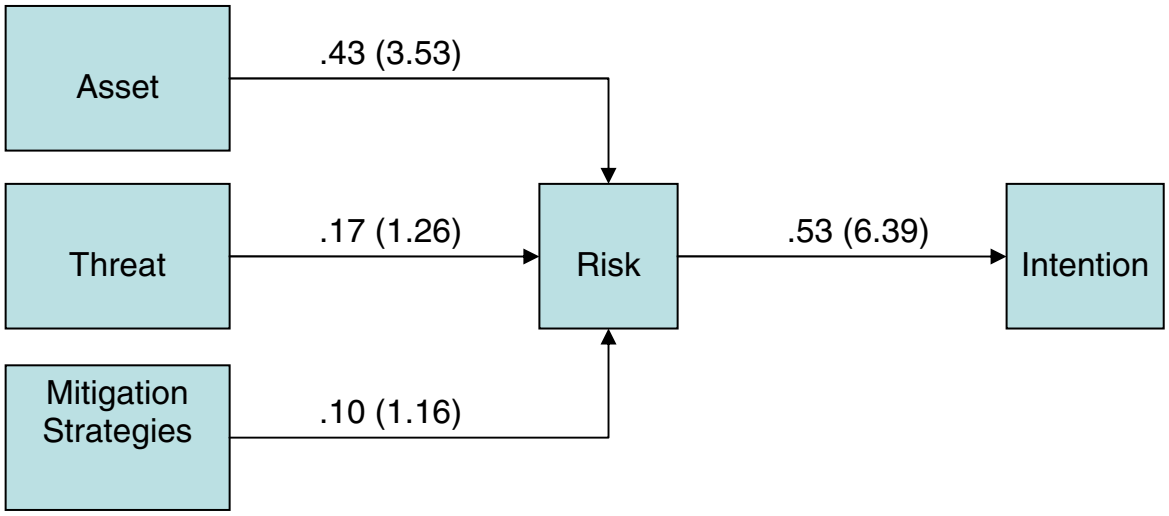

Figure 2: A Test of the Personal Identity Risk Research Model

REFERENCES

1. Anderson, J. and Gerbing, D. (1988) Structural Equation Modeling in Practice: A Review and Recommended Two-Step Approach, *Psychological Bulletin*, 103, 4, 411-423.

2. Ajzen, I. (1991) The Theory of Planned Behavior, *Organizational Behavior & Human Decision Processes*, 50, 179-211.

3. Bagozzi, R. and Yi, Y. (1988) On the Evaluation of Structural Equation Models, *Journal of the Academy of Marketing Science*, 16, 74-97.

4. Berghel, H. (2000) Digital village: Identity theft, social security numbers, and the Web, *Communications of the ACM*, 43, 2, 17-21.

5. Bodin, Lawrence D., Gordon, Lawrence A., and Loeb, Martin P. (2008) "Information Security and Risk Management." *Communications of the ACM*. 51.4, April 2008, pp. 64-68.

6. Chen, J., Schmidt, M., Phan, D. and Arnett, KP. (2008) E-commerce Security Threats: Awareness, Trust, and Practice, forthcoming *International Journal of Information Systems and Change Management*.

7. Dhillon, G. (2007) Principles of Information Systems Security: Text and Cases, John Wiley Publishing, Hoboken, NJ. 2007.

8. Elms, E.R., LaPrade, J.D. and Maurer, M.L. (2008) Hacking of Corporate Information Systems:

Increasing Threats and Potential Risk Management Techniques. *CPCU eJournal*, Feb2008, Vol. 61 Issue 2, p1-9.

9. Federal Trade Commission. (2005) http://www.consumer.gov/idtheft/# (2006) *Consumer Fraud and Identity Theft Complaint Data January – December 2005*. Data from the Sentinel and identity theft clearinghouse.

10. Fornell, C. and Larcker, D. (1981) Evaluating Structural Equation Models with Unobservable Variables and Measurement Error, *Journal of Marketing Research*, 18, 39-50.

11. Garver, M. and Mentzer, J. (1999) Logistics Research Methods: Employing Structural Equation Modeling to Test for Construct Validity, *Journal of Business Logistics*, 20, 1, 33-57.

12. Gefen, D., (2003) "Assessing Unidimensionality through LISREL: An Explanation and Example." *Communications of the Association for Information Systems*, Vol. 12, 2003, pp.23-47.

13. Gefen, D., Karahanna, E. and Straub, D. (2003) Trust and TAM in Online Shopping: An Integrate Model, *MIS Quarterly*, 27, 1, 51-90.

14. Gibbs, Mark. (2008) "Fighting off Strangers Bearing Candy." *Network World*. http://www.networkworld.com/columnists/2008/041708. April 17, 2008.

15. Grant, I. (2007) Salaries for IT risk managers up as threats to continuity drive demand, *Computer Weekly*, 6/26/2007, 48.

16. Grabowski, Martha and Roberts, Karlene H. (1998) "Risk Mitigation in Virtual Organizations." *Journal of Computer-Mediated Communication* 3 (4) 1998.

17. Hines, M. (2006) Insuring against data loss, *EWeek the Enterprise Newsweekly*, 23, 50, December 18/25, 13.

18. Jones, MC, Arnett, KP, Tang, J.-T., and Chen, N.-S. (1993) "Perceptions of Computer Viruses: A Cross-Cultural Assessment," *Computers & Security*, 12, 191-197.

19. Kobsa, Alfred. (2007) "Privacy-enhanced Personalization." *Communications of the ACM*. August 2007, 50.8, pp. 24-33.

20. Krutz Roland L. and Vines, Russel D. (2007) *The CISSP and CAP Prep Guide*. Wiley Publishing, Indianapolis, IN. 2007.

21. LaRose, R., Rifon, N., Liu, S., and Lee, D. (2005) Understanding online safety behavior: A multivariate model, *International Communication Association meeting*, New York, May.

22. Liu, C., Arnett, KP, Beatty, B. and Capella, L.(1997) Fortune 500 Faces the World through Home Pages, *Information and Management*, 31, 335-345.

23. Liu, C., Marchewka, J.T., Lu, J. and Yu, C. (2005) Beyond Concern - a privacy-trust-behavioral intention model of electronic commerce, *Information and Management,* 42, 289-304.

24. Macaulay, T. (2006) Risk Conductors, *Information Systems Security*, 15, 6, 12-24

25. Neumann, P. G. (2003) Information System Security Risk, *Communications of the ACM*, 46, 10, 136.

26. Neumann, Peter G. (2008) Reflections on Computer-Related Risks Communications of the ACM, January 2008, 51.1

27. Okenyi, P.O. and Owens, T.J. (2007) On the Anatomy of Human Hacking, *Information Systems Security*, 16, 6, 302-314.

28. Ortega, R. (2007) Defending the Corporate Crown Jewels from the Dangers that Lurk Within - Effective Internal Network Security Focuses on Behavior, *Information Systems Security*, 16, 1, 54-60

29. Pavlou, P. A. and Fygenson, M. (2006) Understanding and Prediction Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior, *MIS Quarterly*, 30, 1, 115-143.

30. Perez, J.C. (2005) Gartner: Security Concerns to Stunt E-commerce Growth, *ComputerWorld*, June 24.

31. Portz, K., Strong, J.M., Busta, B., and Schneider, K. (2000) Do Consumers Understand What Web Trust Means? *CPA Journal*, 70, 10, 47.

32. Ramsey, E. and McCole, P. (2005) E-business in Professional SMEs: the Case of New Zealand, *Journal of Small Business and Enterprise Development*, 12, 4, 528 – 545.

33. Richardson, R. 2007 CSI Computer Crime and Security Survey. Computer Security Institute. Download available at http://gocsi.com.

34. Saunders, KM (1999) Counteracting identity fraud in the information age: Identity theft and assumption deterrence, *International Review of Law, Computers & Technology*, - Taylor & Francis.

35. Schmidt, MB and Arnett, KP. (2005) Spyware: A Little Knowledge is a Wonderful Thing, *Communications of the ACM*, 48, 8, 67-70.

36. Siemens. (2007). CRAMM Home Page. http://www.cramm.com/

37. Stewart, A. (2004). On risk: perception and direction, *Computers & Security,* 23, 362-370.

38. Straub, D. and Welke, R. J. (1998) Coping With Systems Risk: Security Planning Models for Management Decision Making, *MIS Quarterly*, 22, 4, 441-469.

39. Teo, H., Wei, K. and Benbasat, I. (2003) Predicting Intention to Adopt Interorganizational Linkages: An Institutional Perspective, *MIS Quarterly*, 27, 1,19-49.

40. Thomas, D. (2004) Hack Attacks and Spam Set to Increase, *Computing*, October 7, VNU Business Publications, LTD, London, http://www.computing.co.uk/computing/news/2071100/hack-attacks-spamset-increase, retrieved February 29, 2008.

41. Venkatesh, V., Morris, M. G., Davis, G. B. and Davis, F. D. (2003) User acceptance of information technology: toward a unified view, *MIS Quarterly*, 27, 3, 425-478

42. Wang, F. and Head, M. (2007) How Can the Web Help Build Customer Relationship? An Empirical Study in E-tailing, *Information and Management*, 44, 115-129.

43. Yim, R. A. (2002) National Preparedness: Integrating New & Existing Technology & Information Sharing into an Effective Homeland Security Strategy, 26p, (AN SM195355).

44. Zegans, Leonard. (2008) "Reflections on Computer-Related Risks" Communications of the ACM, January 2008, 51.1, p. 152.

Appendix A – Questionnaire Item Mapping

Measure	Question
AS1	My personal information (e.g. SSN) is valuable to me.
AS2	My user information (address, telephone number, etc.) is important.
AS3	Log-in credentials, such as a password, are important to me.
AS4	Financial information (e.g. credit card number and expiration date) entered for Internet commerce is important to me.
AS5	Personal information that I submit to Internet sites is highly valued to me.
TH1	Malicious code or malware (Viruses, Trojan Horses, Rootkits, Phishing, Pharming, Spyware, etc.) are detrimental to my personal information.
TH2	A hacker could be a menace to my personal information.
TH3	I am concerned about accidental disclosure of my personal information.
TH4	I am concerned about intentional disclosure of my personal information.
TH5	When others spoof (impersonate someone else) my personal information is threatened.
RM1	Weak passwords can allow my identity to be stolen.
RM2	A wireless Internet connection is susceptible to eavesdropping.
RM3	Unencrypted email can allow my identity to be stolen.
RM4	Failing to update my operating system patches can allow my identity to be stolen.
RM5	Failing to update my browser patches can allow my identity to be stolen.
RSK1	If my identity is stolen I could experience financial loss.
RSK2	Identity theft would decrease my trust in information systems.
RSK3	Identity theft would decrease trust in my operating system.
RSK4	Identity theft would decrease trust in my current browser.
RSK5	If my identity were stolen, it would negatively affect my credit rating.
RSK6	If my identity were stolen it would take a lot of time to fix the problem.
INT1	I plan to reduce identity theft by using strong passwords.
INT2	I will attempt to lessen the probability of ID theft by using anti-spyware software.
INT3	I will attempt to prevent ID theft by installing security patches on my operating system.
INT4	I will attempt to prevent ID theft by installing security patches on my Internet Browser.
INT5	I intend to decrease identity theft by not responding to suspicious email.

Appendix B – Correlation Matrix

	AS1	AS2	AS3	AS4	AS5	TH1	TH2	TH3	TH4	TH5	RM1	RM2	RM3	RM4	RM5	RSK1	RSK2	RSK3	RSK4	RSK5	RSK6	INT1	INT2	INT3	INT4	INT5
AS1	1																									
AS2	0.84	1																								
AS3	0.83	0.83	1																							
AS4	0.85	0.76	0.87	1																						
AS5	0.76	0.79	0.78	0.77	1																					
TH1	0.61	0.63	0.64	0.62	0.66	1																				
TH2	0.54	0.52	0.59	0.58	0.67	0.70	1																			
TH3	0.56	0.62	0.59	0.52	0.63	0.68	0.67	1																		
TH4	0.48	0.52	0.49	0.46	0.55	0.60	0.58	0.82	1																	
TH5	0.45	0.44	0.47	0.43	0.48	0.60	0.62	0.64	0.67	1																
RM1	0.59	0.61	0.59	0.58	0.51	0.54	0.44	0.61	0.59	0.52	1															
RM2	0.46	0.48	0.42	0.43	0.42	0.44	0.32	0.46	0.48	0.39	0.60	1														
RM3	0.41	0.45	0.40	0.42	0.43	0.41	0.41	0.41	0.49	0.52	0.51	0.62	1													
RM4	0.38	0.41	0.39	0.35	0.42	0.36	0.35	0.47	0.47	0.51	0.54	0.57	0.76	1												
RM5	0.50	0.53	0.49	0.47	0.49	0.46	0.36	0.55	0.52	0.54	0.58	0.63	0.71	0.88	1											
RSK1	0.70	0.59	0.68	0.73	0.62	0.53	0.53	0.52	0.40	0.42	0.60	0.42	0.41	0.35	0.43	1										
RSK2	0.48	0.50	0.51	0.53	0.51	0.36	0.43	0.32	0.35	0.40	0.38	0.32	0.40	0.30	0.29	0.54	1									
RSK3	0.48	0.52	0.50	0.51	0.48	0.38	0.40	0.36	0.40	0.48	0.34	0.34	0.39	0.28	0.36	0.40	0.72	1								
RSK4	0.45	0.49	0.48	0.50	0.47	0.36	0.45	0.36	0.35	0.41	0.35	0.30	0.39	0.33	0.35	0.39	0.77	0.85	1							
RSK5	0.53	0.50	0.55	0.62	0.55	0.47	0.46	0.43	0.38	0.44	0.50	0.40	0.33	0.29	0.42	0.61	0.41	0.46	0.46	1						
RSK6	0.66	0.61	0.63	0.69	0.59	0.48	0.47	0.42	0.38	0.45	0.49	0.39	0.33	0.31	0.42	0.66	0.52	0.51	0.53	0.80	1					
INT1	0.58	0.60	0.61	0.58	0.52	0.42	0.32	0.48	0.40	0.36	0.65	0.47	0.46	0.46	0.51	0.50	0.34	0.39	0.35	0.50	0.49	1				
INT2	0.49	0.51	0.54	0.53	0.50	0.42	0.44	0.51	0.41	0.43	0.50	0.38	0.43	0.43	0.39	0.50	0.37	0.41	0.41	0.45	0.42	0.70	1			
INT3	0.35	0.37	0.42	0.41	0.46	0.35	0.37	0.40	0.35	0.34	0.43	0.41	0.40	0.52	0.44	0.38	0.32	0.26	0.32	0.40	0.36	0.60	0.75	1		
INT4	0.23	0.24	0.14	0.26	0.26	0.20	0.20	0.25	0.21	0.03	0.28	0.21	0.20	0.29	0.30	0.24	0.20	0.17	0.21	0.26	0.24	0.37	0.20	0.30	1	
INT5	0.69	0.61	0.66	0.68	0.59	0.58	0.48	0.47	0.40	0.38	0.48	0.37	0.29	0.30	0.40	0.57	0.42	0.41	0.39	0.51	0.57	0.66	0.63	0.57	0.33	1