2010

Utilizing the Technology Acceptance Model to Assess the Employee Adoption of Information Systems Security Measures

Cynthia M. Jones
Nova Southeastern University

Richard V. McCarthy
Quinnipiac University

Leila Halawi
Quinnipiac University, halawil@erau.edu

Bahaudin Mujtaba
Nova Southeastern University

UTILIZING THE TECHNOLOGY ACCEPTANCE MODEL TO ASSESS THE EMPLOYEE ADOPTION OF INFORMATION SYSTEMS SECURITY MEASURES

Cynthia M. Jones, Nova Southeastern University, x2cjones@yahoo.com
Richard V. McCarthy, Quinnipiac University, richard.mccarthy@quinnipiac.edu
Leila Halawi, Quinnipiac University, leila.halawi@quinnipiac.edu
Bahaudin Mujtaba, Nova Southeastern University, mujtaba@huizenga.nova.edu

ABSTRACT

In this study, the factors that affect employee acceptance of information systems security measures were examined by extending the Technology Acceptance Model. Partial least squares structural equation modeling was applied to examine these factors. 174 valid responses from employees from companies in various industry segments in the United States and Canada were analyzed. The results of the statistical analysis indicate that subjective norm moderated by management support showed the strongest effect on intention to use information systems security measures.

Keywords: Technology Acceptance Model (TAM), Information Systems Security, Partial Least Squares

INTRODUCTION

Companies are increasing their investment in technologies to enable better access to information and to gain a competitive advantage. Global competition is driving companies to reduce costs and enhance productivity, increasing their dependence on information technology. Information is a key asset within an organization and needs to be protected. Expanded connectivity and greater interdependence between companies and consumers has increased the damage potential of a security breach to a company's information systems. Improper unauthorized use of computer systems can create a devastating financial loss even to the point of causing the organization to go out of business. It is critically important to understand what causes users to understand, accept and to follow the organization's information systems security measures so that companies can realize the benefits of their technological investments. In the past several years, computer security breaches have stemmed from insider misuse and abuse of the information systems and non-compliance to the information systems security measures. The purpose of this study was to address the factors that affect employee acceptance of information systems security measures.

This article discusses the information systems security measures and explains the Technology Acceptance Model (TAM). This is followed by a presentation of the methodology and the results of the statistical analysis. The article closes with a discussion of the conclusions, implications and contribution of this research.

INFORMATION SYSTEMS SECURITY MEASURES

Companies are becoming increasingly vulnerable to both internal and external threats to their information systems. These threats are categorized as computer crime. With the increasing threat of computer crime, information technology security has become of great concern to companies. As businesses operate in the global arena, it has become vitally important to guard and protect information and the computer assets from computer crimes. Based on recent studies and reported incidents, the threat of computer crime is real and increasing. More incidents of computer crime are being reported each year and criminals are becoming more sophisticated in their attacks (Mujtaba, Griffin, & Oskal, 2004).

In 2005, a five-year industry analysis showed a gradual rise in the number of security incidents, with 34% of companies reporting one to five security breaches in 1999 and 47% reporting one to five breaches in 2004 (Emrich, 2005). In 2006, losses due to security breaches were reported to be over $52 million for the 313 respondents that were willing and able to estimate losses (Gordon et al., 2006). The 2006 CSI/FBI survey estimated the average loss per the 313 respondents was $167,713 (Gordon et al., 2006). Companies are vulnerable to both external and internal attack. According to research conducted by Gartner, Inc. in 2006, the cost of recovery from a security breach can be up to 15 times greater than the cost of prevention by protecting the data in the first place. A company with 10,000 customer accounts can spend $6 to $16 dollars per customer on data encryption and intrusion detection and prevention as

compared to $90 per customer account when a data breach occurs (anonymous, 2006).

The human factor has been considered the weakest link in the security solution or at a minimum it plays a critically important role in the protection of information and information systems. If users are unwilling to accept security measures and systems, the systems will not bring the full benefits of the technology to the organization (Venkatesh & Davis, 1996).

The perpetrator of a cybercrime is increasingly being identified as an employee, rather than an unknown hacker (Mujtaba et al., 2004). In 2006, a survey of technology, media and telecommunication firms, the biggest threats were identified as employees sending out information through email to unauthorized users (67%), employee misconduct (57%) and theft of intellectual property (52%) (Deloitte, 2006). For financial services institutions, 49% of the respondents indicated that they had experienced an internal security breach. Of these breaches 31% were from viruses and worms introduced internally, 28% were from insider fraud and 18% were leaks of customer data by insiders (Deloitte, 2006). In the 2007 survey of financial institutions, 31% experienced security breaches due to employee misconduct (Deloitte, 2007). In the technology, media and telecommunication firms survey and the financial institutions survey conducted by Deloitte in 2007, 91% of the respondents considered employee misconduct a major concern (Deloitte, 2007).

According to the 2006 CSI Computer Crime and Security survey, most of the organizations believed that insiders accounted for a substantial portion of the losses. Sixty-nine percent of the respondents attributed the financial losses to insiders (Gordon et al., 2006). According to a Datamonitor study in 2007, the respondents indicted that most of the security incidents were the result of unintentional mistakes, however, 23% of the breaches were considered to be malicious actions taken by employees (Hall, 2007). In the 2007 CSI Survey, 64% of the respondents reported that a percentage of the losses were due to insider threats, mostly stemming from abuse of network resources (Richardson, 2007). The 2008 CSI Computer Crime and Security Survey reported that insider abuse of network was the second most frequent type of security breach behind virus incidents (Richardson, 2008).

Managers must understand that threats of computer crime in the form of information breaches are real and they must ensure that appropriate information security strategies, policies, procedures, and measures are in place, communicated to employees and enforced throughout the organization. Destruction or loss of information or information systems could seriously affect the company's bottom line as well as the company's market share and corporate reputation. The impact of cybercrime could be even more severe if the corporate information is sold or given to competitors from hackers or disgruntled employees.

Given the large negative impact on the company's goals and finances, companies must develop mechanisms to better measure the impact of information technology breaches, and more importantly, companies need to develop an information security strategy and invest in information systems security measures to protect their corporate information. These measures must include investment in physical information technology security, such as firewalls and virus protection software as well as documentation and training of employees in the information security polices and practices. Senior management must take an active role in developing this strategy and communicating it throughout the organization. Management support and training support have been shown to positively influence technology acceptance (Schepers, Wetzels, & de Ruyter, 2005; Peltier, 2005; Myler & Broadband, 2006).

TECHNOLOGY ACCEPTANCE MODEL

The Technology Acceptance Model has been adapted from the Theory of Reasoned Action regarding beliefs, attitude, intention and behavior for modeling user acceptance of information systems (Davis, Bagozzi & Warshaw, 1989). The Theory of Reasoned Action is a social psychology model that examines the key determinants of intended behaviors. According to the model, an individual's performance of a particular behavior is determined by his or her behavioral intention to perform the behavior and behavioral intention is determined by multiple factors including a person's attitude and subjective norms (Davis et al., 1989).

The basic premise of the Technology Acceptance Model is that the more accepting users are of new systems, the more they are willing to make changes in their practices and use their time and effort to actually start using the system. Davis (1989) posited that the perceptions of ease of use and usefulness were key indicators of consumer's intention to adopt a new technology. Perceived usefulness referred to the tendency to use or not to use a technology to the

extent it is believed that it will help or enhance an individual's ability to perform his or her job better. Perceived ease of use involved the level of effort it would take to use an application such that the degree a person believes a system is free of effort, he or she would be more likely to use and accept the system. Perceived ease of use also influenced perceived usefulness in that the easier the system is perceived to be to use, the more useful it would be (Davis, 1989). Actual system use is determined by perceived usefulness and perceived ease of use, which is related to attitudes towards use, which in turn, relates to intention and finally to behavior. Davis and Venkatesh (1996) developed the Parsimonious Technology Acceptance Model as shown in Figure 1, which excluded attitude as a construct because based on empirical studies which indicated that attitude did not fully mediate the effect of perceived usefulness on intention.

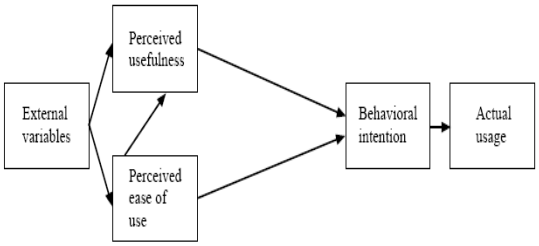

Figure 1. Parsimonious Technology Acceptance Model (Davis & Venkatesh, 1996)

The Technology Acceptance Model has been established and replicated through the study of many applications (Davis & Venkatesh, 1996; Venkatesh & Morris, 2000). Most of the body of research on the technology acceptance model has been based on voluntary intention and use of systems and technology. Brown, Massey, Montoya-Weiss and Burkman (2002) tested the model where behavior and use of a system or technology was mandated for individuals to keep and perform their jobs. They found the basic relationships of the model were still maintained even though the weightings varied from those in a volitional environment. This is particularly important in the adoption of information systems security measures since in most cases, use of information systems security measures is mandatory.

RESEARCH QUESTIONS

The research problem that was addressed in this study is to determine what the key behavioral factors were that affect an employee's acceptance of information systems security measures. The specific research questions that were addressed included:

Do the employee perceptions regarding the information systems security measures in an organization affect the intention to use information systems security measures?

Do the beliefs of others about the use of information systems security measures affect employee perceptions and the intention to use information systems security measures?

Does management support affect user perceptions and the intention to use information systems security measures?

METHODOLOGY

The parsimonious Technology Acceptance Model was extended to examine the employee adoption of security measures. The model and the relationship paths are shown in Figure 2. The independent variables in the model were perceived usefulness, perceived ease of use, and subjective norm. The dependent variable was intention to use the information systems security measures.

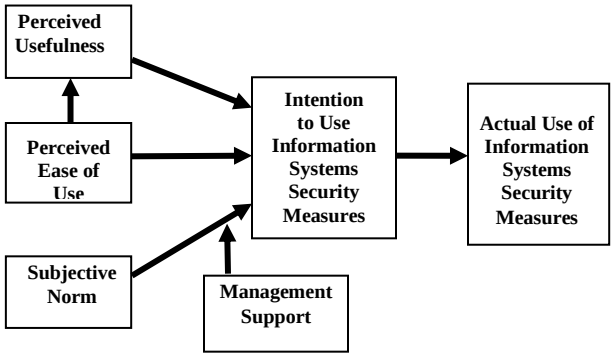

Figure 2. Research Model

The hypotheses that were examined in this study included:

H_1: There is a positive relationship between perceived usefulness and the intention to use information systems security measures.

H_2: There is a positive relationship between perceived ease of use and intention to use information systems security measures.

H_3: There is a positive relationship between perceived ease of use and perceived usefulness related to the use of information systems security measures.

H_4: There is a positive relationship between subjective norm and the intention to use information systems security measures.

H_5: The relationship between subjective norm and intention to use will attenuate with increased management support.

A questionnaire was developed to gather data to test the hypotheses. The theoretical constructs were operationalized and measured using items derived from validated surveys from previous research. Multi-item scales were used based on previously published scales and adapted for the current context (Venkatesh & Davis, 2000). The questions were modified to fit the context of the study.

The questionnaire was formatted using the electronic survey tool, Survey Monkey. A link to the survey was distributed to potential respondents via email. The target sample population was employees who work at companies that have information systems security measures. The employees worked in various industry segments and geographical locations within the United States and Canada. The companies varied in size in terms of numbers of employees from small to very large.

A convenience sampling using personal contacts was used to select subjects. Snowball sampling was also used whereby the initial subjects were requested to generate additional subjects. There were 174 completed questionnaires obtained for analysis.

ANALYSIS OF RESULTS

Partial least squares using Smart PLS was used to analyze the data and test the hypotheses. PLS recognizes two models: the measurement model and the structural model.

Assessing the Measurement Model

The measurement model consists of relationships among the conceptual factors and the measures underlying each construct (Ifinedo, 2006; Halawi & McCarthy, 2008). It is assessed by examining individual item reliabilities, internal consistency and discriminant validity. It is necessary to test that the measurement model has a satisfactory level of validity and reliability before testing for a significant relationship in the structural model (Fornell & Larcker, 1981; Ifinedo, 2006).

Reliability measures the degree to which the set of indicators of a latent variable is internally consistent in their measurements (Hair, Black, Babin, Anderson & Tatham, 2006). As shown in Table 1, the value of the composite reliability of the different latent variables ranged from 0.89 to 0.960. These values exceeded the recommended acceptable limit of 0.70, indicating reliability.

Table 1 Composite Reliability

Construct	Composite Reliability
Intention to Use	0.96
Management Support	0.90
Perceived Ease of Use	0.92
Perceived Usefulness	0.95
Subjective Norm	0.94

Another measure to assess reliability and consistency of the entire scale is Cronbach's Alpha. Cronbach's Alpha can also be used to quantify unidimensionality, which means that a set of measured indicators have only one underlying construct (Hair et al., 2006). Table 2 shows the values of Cronbach's Alpha, which range from .83 to .94 for the latent variables. These values exceeded the threshold of 0.70 to indicate reliability.

Table 2 Cronbach's Alpha

Latent Variable	Cronbach's Alpha
Intention to Use	0.94
Management Support	0.83
Perceived Ease of Use	0.90
Perceived Usefulness	0.94
Subjective Norm	0.90

Validity is the extent to which a scale or set of measures accurately represents the concept. Ifinedo (2006) indicated that the two main dimensions for testing the measurement model were convergent validity and discriminant validity. The average variance extracted (AVE) measures convergent validity. Fornell and Larcker (1981) recommended values higher than 0.50 to indicate convergent validity. Table 3 shows the average variance extracted for each latent variable. The values were greater than the .50 threshold indicating convergent validity.

Table 3 Average Variance Extracted

Latent Variable	AVE
Intention to Use	0.86
Management Support	0.75
Perceived Ease of Use	0.67
Perceived Usefulness	0.77
Subjective Norm	0.83

Discriminant validity is the extent a construct or variable is distinct from another variable or construct (Hair et al., 2006). Table 4 shows the average variance extracted, the latent variable correlations and the square root of the average variance extracted. The square root of the average variance extracted is shown on the diagonal of the table. No correlations were equal to or greater than the square root of the average variance extracted indicating there was discriminant validity.

Table 1 Latent Variable Correlations

Construct	INT	MG	PEOU	PU	SN
Intention to Use	.93				
Management Support	.84	.86			
Perceived Ease of Use	.48	.39	.82		
Perceived Usefulness	.29	.24	.65	.88	
Subjective Norm	.70	.67	.43	.41	.91

Assessing the Structural Model

The structural model gives information as to how well the theoretical model predicts the hypothesized paths or relationships (Ifinedo, 2006). It is estimated by the path coefficients and the size of the R-squared values. Smart PLS provides the squared multiple correlations (R-squared) for the endogenous construct in the model and the path coefficients. R-squared indicates the percentage of the variance of the constructs in the model. The path coefficients indicate the strengths of relationships between constructs (Chin, 1998). The values of the path coefficients and R-squared are shown in Figure 3.

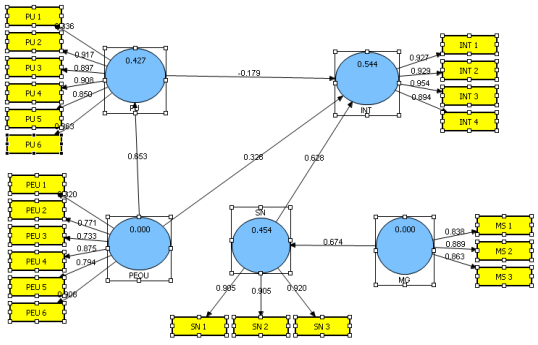

Figure 3. Structural Model

As hypothesized, perceived ease had a positive and moderate effect on intention to use with a path coefficient of .33. Also as hypothesized subjective norm had a positive and significant effect on intention to use with a path coefficient of .63. The constructs of perceived ease of use and subjective norm account for 54% of the variance in intention to use in the model. Inconsistent with the hypothesis 1, perceived usefulness had a negative effect on intention to use.

Consistent with hypothesis 2, perceived ease of use had a positive and significant effect on perceived usefulness. The path coefficient was .65. It accounted for 43% of the variance of perceived usefulness. Management support had a significant and positive effect on subjective norm. The path coefficient was .67. It accounted for 45% of the variance of subjective norm.

The test of significance of all paths was done using the bootstrap re-sampling procedure with 200 re-samples. The test statistic indicates if the relationship is statistically different than zero. Table 5 shows the values of the test statistic.

Table 5 Test Statistics

	T Statistics (|O/STERR|)
MG -> INT	3.16
MG -> SN	7.56
PEOU -> INT	1.53
PEOU -> PU	8.59
PU -> INT	1.06
SN -> INT	4.68

The t values need to be significant to support the hypothesized paths (1.96 or 2.56 for alpha level of 0.05 or 0.001). The bootstrapping results were applied to each of the hypotheses with the null hypothesis not being rejected for Hypothesis 1 and Hypothesis 2. , The null hypotheses 3, 4 and 5 were rejected..

CONCLUSIONS

The objective of this study was to propose and test a research model to evaluate employee acceptance of information systems security measures. The theoretical framework for the study was the Technology Acceptance Model by Davis et al., (1989). The parsimonious model was used and customized to suit the context of information systems security.

Most of the literature would suggest perceived usefulness has a positive and significant relationship with intention to use. In most studies, this relationship between perceived usefulness and intention to use was found to have a greater degree of significance than other variables (Davis et al., 1992; Adams, Nelson & Todd, 1992; Barnett, Kellermanns, Pearson & Pearson, 2006/2007; Szajna, 1996; Koufaris, 2002; Gong, Xu, & Yu, 2004). In mandatory settings however perceived ease of use was shown to have a greater degree of significance on intention to use than perceived usefulness on intention to use (Brown et al., 2002; Adamson & Shine, 2003; Nah, Tan, & Teh, 2004).

Use of the computer information systems security measures served as the context of this study. In most organizations, the use of the computer information systems security measures is mandatory. Contrary to the literature, hypothesis H_1 and hypothesis H_2 were not supported. Perceived usefulness and perceived ease of use were not found to have a strong effect on intention to use computer information security measures. In the context of security, organizations may be more focused on protecting themselves against the vulnerabilities of computer information systems attacks rather than being concerned over how the employees perceived the usefulness or ease of use of the security measures. The organizations may intentionally have made the security measures more difficult to use as a greater defense against attacks.

Indicated in past empirical research, perceived ease of use had a positive and significant relationship with perceived usefulness (Davis, 1989; Davis et al., 1993; Igbaria, Guimaraes, & Davis, 1995; Szajna, 1996; Fagan, Neill, & Woolridge, 2008). Hypothesis H_3 was supported in this study. Perceived ease of use was found to have a strong effect on perceived usefulness.

Melone (1990) and Hartwick and Barki (1994) contended that subjective norm would have a positive and significant impact on intention to use in mandatory settings. The hypothesis H_4 was supported in this research. Subjective norm was found to have a strong effect on intention to use the computer information systems security measures.

Management support and training support have been shown to positively influence technology acceptance (Schepers et al., 2005; Peltier, 2005; Myler & Broadband, 2006). Hypothesis H_5 was supported in that management support had a very strong impact on subjective norm which attenuated the impact on intention to use the computer information systems security measures.

The results of this research will help senior managers and middle level management understand the factors that promote employee adoption, use and compliance with the corporate information systems security measures and to encourage positive attitudes toward these measures. The ability to promote adoption of information systems and the associated security measures will help firms better achieve the benefits of technology within the organization. Widespread employee adoption of the information systems and security measures should have a material financial benefit.

Information systems security management has been identified as the chief concern on the list of top ten technology concerns and initiatives identified by the American Institute of Certified Public Association in 2007 (Deloitte, 2007). It is required to protect data and systems with the increase in system connectivity and information exchange between employees, suppliers and customers. Information systems security is no longer simply a technical issue. Development of an information systems security strategy and the implementation of information systems security controls need to take into account the business goals and objectives of the organization. These strategies and controls need to include a security vision and strategy, senior management commitment, an information systems security management structure and training (Ezingeard, McFadzean, & Birchall, 2005; Hazari, 2005; Peltier, 2005). This empirical research indicates that employees do not perceive the information systems security measures to be easy to use or useful. The research would indicate that there is a need for management to be involved in the creation of the security strategy and to actively communicate the strategy to employees. Given the significant effect of subjective norm on intention to use the information systems security measures, it is critical for supervisors and senior management to emphasize to employees the importance of complying with the company's information systems security measures. It may be beneficial for organizations to consider simplifying the information security processes to encourage the proper use of the information systems security measures.

Limitations of this Study

There were a few limitations of this study which may have affected the results. First, the data collection procedure used did not allow an accurate count as to

the number of respondents to the survey. Further, some of the respondents may not have matched the target population since the snowballing technique was used. This may not have been issue since no outliers were found in the responses. Only employees who worked in companies in the United States and Canada were intended to participate in the study. There was no practical way to know if the respondents were from the Unites States or Canada. Self-reported data was used in this study, which often create a concern because individuals sometimes have difficulty rating their behavior accurately. Self-reported data cannot control for the possibility that a participant gives perceived desirable answers versus the most truthful answers.

Recommendations for Future Research

Based on the results of this study, it may be useful to conduct an empirical research using the original Technology Acceptance Model to take into account the employee's attitudes. An employee's attitude about his or her peers, supervisors and/or the job may affect the employee's intention to follow the information systems security measures. Another recommendation is to conduct an empirical study using the Theory of Planned Behavior as the theoretical framework since subjective norm and attitude are key constructs in this theory and subjective norm was shown to have the strongest effect on intention in this study. Research examining demographics to determine if there are similarities or differences in employee acceptance of computer information systems security measures based on gender, years of employment, management level and age may provide additional insights into promoting employee acceptance and use of computer information systems security measures.

REFERENCES

Adams, D., Nelson, R., & Todd, P. (1992). Perceived usefulness, ease of use, and usage of information technology: A replication. *MIS Quarterly, 16*(2), 227-247.

Adamson, I., & Shine, J. (2003). Extending the new technology acceptance model to measure the end user information systems satisfaction in a mandatory environment: a bank's treasury. *Technology Analysis and Strategic Management, 15*(4), 441-455.

Anonymous. (2006). www.RIMS.org/riskwire. *Risk Management, 53*(9), 8-9.

Barnett, T., Kellermanns, F., Pearson, A., & Pearson, R. (2006/2007). Measuring information system usage: Replication and extensions. *The Journal of Computer Information Systems, 47(*2), 76-85.

Brown, S., Massey, A., Montoya-Weiss, M., & Burkman, J. (2002). Do I really have to? User acceptance of mandated technology. *European Journal of Information Systems, 11*, 283-295.

Chin, W. W. (1998). Issues and opinion on structural equation modeling. *MIS Quarterly, 22*(1), 7-16.

Davis, F. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319-340.

Davis, F., Bagozzi, R., & Warshaw, P. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, *35*(8), 982-1003.

Davis, F. & Venkatesh, V. (1996). A critical assessment of potential measurement biases in the technology acceptance model: three experiments. *International Journal Human-Computer Studies, 45*, 19-45.

Deloitte. (2006). 2006 global security survey. 1-44.

Deloitte. (2006). Protecting the digital assets: the 2006 technology, media, and telecommunications security survey. 1-16.

Deloitte. (2007). Treading water: The 2007 technology, media & telecommunications security survey. 1-42.

Deloitte. (2007). 2007 global security survey: The shifting security paradigm. 1-46.

Emrich, A. (2005). Information security poses increasing problems. *Grand Rapids Business Journal*, *23*(11), 10.

Ezingeard, J., McFadzean, E., & Birchall, D. (2005). A model of information assurance benefits. *EDPACS, 32*(11), 1-16.

Fagan, M., Neill, S., & Woolridge, B. (2008).

Exploring the intention to use computers: An empirical investigation of the role of intrinsic motivation, extrinsic motivation and perceived ease of use. *Journal of Computer Information Systems, 48*(3), 31-37.

Fornell, C., & Larcker, D. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39-50.

Gong, M., Xu, Y., & Yu, Y. (2004). An enhanced technology acceptance model for web-based learning. *Journal of Information Systems Education, 15*(4), 365-374.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2006). *2006 CSI/FBI Computer Crime and Security Survey*. San Francisco: Computer Security Institute.

Hair, J., Black, W., Babin, B., Anderson, R., & Tatham, R. (2006). *Multivariate Data Analysis*. Upper Saddle River, New Jersey: Pearson Prentice Hall.

Halawi, L., & McCarthy, R. (2008), Measuring Student Perceptions of Blackboard Using the Technology Acceptance Model: A PLS Approach, *Issues in Information Systems*, *9*(2), 95-102.

Hall, M. (2007). On the mark. *Computerworld, 41*(18), 11.

Hartwick, J., & Barki, H. (1994). Explaining the role of user participation in information system use. *Management Science, 40*(4), 440-465.

Hazari, H. (2005). Perceptions of the end-users on the requirements in personal firewall software: An exploratory study. *Journal of Organizational and End User Computing, 17(*3), 47-65.

Ifinedo, P. (2006). Acceptance and continuance intention of web-based learining technologies (WLT) use among university students in a Baltic country. *The Electronic Journal on Information Systems in Developing Countries, 23*(6), 1-20.

Igbaria, M., Guimaraes, T., & Davis, G. B. (1995). Testing the determinants of microcomputer usage via a structural equation model. *Journal of Management Information Systems, 11*(4), 87-114.

Koufaris, M. (2002). Applying the technology acceptance model and flow theory to online consumer behavior. *Information Systems Research, 13*(2), 205-223.

Melone, N. (1990). A theoretical assessment of user-satisfaction construct in information systems research. *Management Science, 36*(1), 76-91.

Mujtaba, B., Griffin, C., & Oskal, C. (2004). Emerging ethical issues in technology and countermeasures for management and leadership considerations in the twenty first century's competitive environment of global interdependence. *Journal of Applied Management and Entrepreneurship*, *9*(3), 1-17.

Myler, E. & Broadbent, G. (2006). ISO 17799 : Standard for security. Information *Management Journal, 40*(6), 43-52.

Nah, F., Tan, X., & Teh, S. (2004). An empirical investigation on end-users' acceptance of enterprise systems. *Information Resources Management Journal, 17*(3), 32-53.

Peltier, T. (2005). Implementing an Information Security Awareness Program. *EDPACS*, 33 (1), 1-19.

Richardson, R. (2008). 2008 CSI Computer crime and security survey. Computer Security Institute, 1-30.

Richardson, R. (2007). 2007 CSI Computer crime and security survey. Computer Security Institute, 1-29. Retrieved from www.gocsi.com.

Schepers, J., Wetzels, M., & de Ruyter, K. (2005). Leadership styles in technology acceptance: Do followers practice what leaders preach? *Managing Service Quality, 15*(6), 496-508.

Szajna, B. (1996). Empirical evaluation of the revised technology acceptance model. Management Science, 42(1), 85-92.

Venkatesh, V., & Davis, F. (1996). A model of the antecedents of perceived ease of use: Development and test. *Decision Sciences, 27*(3), 451-481.

Venkatesh, V. & Morris, M. (2000). Why don't men ever stop to ask for directions? Gender, social influences and their role in technology acceptance and usage behavior. *MIS Quarterly, 24*(1), 115-139.