Journal of International Technology and Information Management

Volume 19 | Issue 3 Article 2

2010

Evaluating the Perceived Impact of Collaborative Exchange and Formalization on Information Security

Randall Young
University of Texas

Evaluating the Perceived Impact of Collaborative Exchange and Formalization on Information Security

Randall Young
University of Texas – Pan American
USA

ABSTRACT

Organizations integrate information security measures through information security planning and policy development. This study aims to examine how the extent of collaborative exchange within the organization and extent of formalization of the information security function impact the effective utilization of well-established information security objectives. The security objectives of interest, described in general deterrence theory, are deterrence, detection and recovery. This study finds that organizations that exhibit higher levels of collaborative exchange and develop and implement more information security policies are more effectively utilizing the information security strategies of detection, deterrence and recovery. This study highlights the importance of the complementary nature of collaborative exchange and formalization within the information security discipline.

INTRODUCTION

Today, in large part, information security is the implementation of controls and best practices suggested by consultants, standard governing bodies (i.e. National Institute of Standards & Technology) (NIST), International Organization for Standardization / International Electrotechnical Commission (ISO/IEC), etc.), the organization's information security department and, sometimes, the organization's employees. While the use of global standards of practice, top management and the information security department within the organization to guide information security planning and implementations may be useful, existing research consistently shows a positive relationship exists between user involvement in planning and the effectiveness of the information systems function within organizations (Gottschalk, 1999; Sambamurthy et al., 1994; Segars & Grover, 1998). A deliverable of the information security planning process is the organization's information security policies and procedures. Standard governing bodies (NIST, ISO/IEC) and researchers (Bidgoli, 2003; Garrison & Posey, 2006) stress the importance of creating information security policies and provide guidance on the different types of information security policies that an organization may need.

This research attempts to examine the impact of end-user involvement and formalized information security policies on the effectiveness of the information security function within organizations. Specifically, this study focuses on two antecedent variables, collaborative exchange and formalization, and how it impacts the effective utilization of the information security strategies of deterrence, detection and recovery. Collaborative exchange is an assessment of the extent of collaboration between upper-level management, end users and the information security function. Formalization is an assessment of the extent of established formal information security policies within an organization.

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

The purpose of this research is twofold. First, this research aims to examine the individual effects of formalization and collaborative exchange on the effectiveness of information security detection, deterrence, and recovery activities. Much of the effort expended in the management of information security is in developing and enforcing information security policies. By examining formalization separately, the impact of information security policy development on effective utilization of information security strategies can be assessed. The second aim of this research is to examine the impact of collaborative exchange and formalization in concert on the effectiveness of information security detection, deterrence, and recovery activities. Evaluating complementary effect of collaborative exchange and formalization on effective utilization of information security strategies provides evidence supporting the importance of establishing information security policies with input and effort from all major constituencies within the organization.

This study makes several contributions to the literature and practice. First, this research provides insight into how management choices in regards to establishing formal communication channels and developing information security policies may impact the effectiveness of the information security function. Second, the presence of the dependent variable, effectiveness of detection, deterrence and recovery activities, gives academics and practitioners a success measure which can guide more effective decision making in the information security domain.

The remainder of this manuscript is organized as follows. The next section discusses the literature supporting the constructs of interest in this study. The following two sections will present the methodological approach taken in this study and the results of data collection. The next section will present the efforts in data analysis. The last section will present a discussion of the important findings and limitations of this research.

RESEARCH PROBLEM DEVELOPMENT

Collaborative exchange and formalization

Top management support and involvement has been identified as a significant factor impacting the success, or lack thereof, of IT projects and investments (Byrd et al., 1995; Hartono et al., 2003; Jitpaiboon & Kalaian, 2005; Lederer & Salmela, 1996; Premkumar & King, 1994; Sasidharan et al., 2006). There is no such thing as perfect security. As a result, every organization must identify the value of the information assets within the organization and determine an acceptable level risk. Not all information assets in the organization are equal and, as such, determining acceptable levels of security expenditures and controls for each major information asset should not be the same. After identifying the major type of information assets and their relative worth to the organization, a decision about acceptable risk levels for each information asset should be made and senior management is in the best position to make this decision (Dutta & McCrohan, 2002).

The assumption that organizations have clear-cut, stable organizational goals is likely inaccurate for many organizations (Lederer & Sethi, 1992; Premkumar & King, 1994). Research has shown that the organizational goals are established through a dynamic, politically-charged process that results in temporary stability (King & Kraemer, 1984). Through active participation in the

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

business planning process, the information security executive acquires a more enterprise-level view of the organization and has less trouble understanding top management's objectives and strategic decisions allowing them to develop more useful relevant information security plans (Lederer & Mendelow, 1987). Information security plans not linked to organizational goals and strategy are viewed as lacking relevance leading to poor utilization of resources and implementation problems which impact the effectiveness of the information security function (Sabherwal, 1999). As such, organizations with strong collaborative exchange behaviors between upper-level management and information security function are expected to manage information security more effectively.

The users have been consistently viewed as the weak link in the information security literature (Schultz et al., 2001; Wade, 2004). Leaving them out of the planning process has the potential to alienate the information users which could lead to conflict during plan implementation and lasting discord between the users and the information security department (Brancheau et al., 1989). An environment of discord is certainly at odds with the ideals of a collaborative, knowledge-sharing organization. While traditional information security evaluation methods are heavily focused on quantitative costs and benefits and ignore qualitative issues (Bodin et al., 2005), newer information security standards (published by the Government Accountability Office & National Institute of Standards & Technology) are pushing for more use of qualitative information to make information security decisions. High quality information is critical in evaluation methods that evaluate qualitative information (Blakley et al., 1991) and the knowledge of vulnerabilities, threats, and risk that make up the organization's environment are not exclusively or conclusively known at the executive level (James, 1996; Pattinson & Anderson, 2007). Ultimately it is the users who must abide by and use the prescriptions that make up the finalized information security plan. As such, an organization that nurtures and encourages collaborative exchange between management, end users and the information security function is theorized to manage information security is a more effective manner.

The literature identifies a number of benefits gained through better communication and collaboration which include improved top management commitment (Teo & Ang, 2001), higher visibility of the information security function (Chi et al., 2005), more aligned business and security plans (Byrd et al., 1995; Lederer & Sethi, 1992), fewer implementation problems (Premkumar & King, 1994), better utilization of resources (Sabherwal, 1999), and higher user acceptance (James, 1996; Pattinson & Anderson, 2007). This leads to the first set of hypotheses below.

H_{a1a}: Collaborative exchange will positively impact the effectiveness of information security detection measures.

H_{a1b}: Collaborative exchange will positively impact the effectiveness of information security deterrence measures.

H_{a1c}: Collaborative exchange will positively impact the effectiveness of information security recovery measures.

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

Formalization or standardization is the presence of written rules, policies, and procedures that drive the behavior of people within an organization. Previous research has examined the formalization or standardization of organizational functions using such measures as the number of written rule, policies and procedures in place and the extent to which these written documents are used (Zmud, 1982; Zollo & Winter, 2002). Formalization has been shown in previous research to increase user's perception in regards to the importance of performing the respective tasks (Jansen et al, 2006; Zmud, 1982). The last three hypotheses are described below.

H_{a2a}: More formalized information security programs are positively associated with higher levels of effectiveness of information security detection measures.

H_{a2b}: More formalized information security programs are positively associated with higher levels of effectiveness of information security deterrence measures.

H_{a2c}: More formalized information security programs are positively associated with higher levels of effectiveness of information security recovery measures.

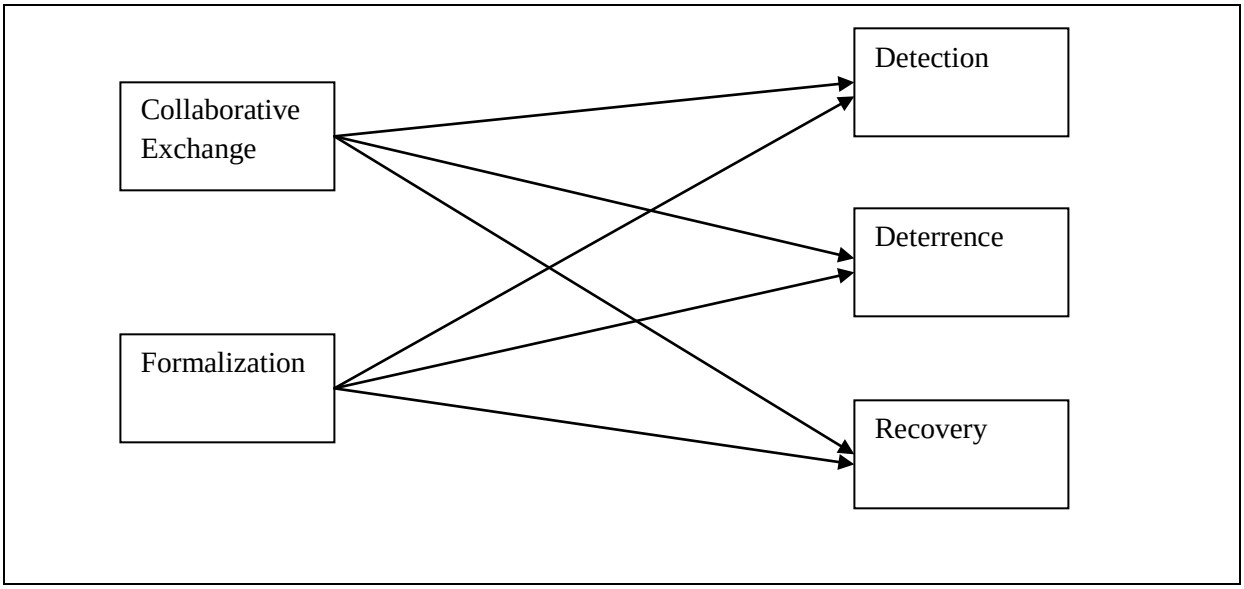
METHOD

Figure 1 shows the full research model which encompasses five constructs of interest: collaborative exchange, formalization, information security detection strategies, information security deterrence strategies and information security recovery strategies. The difficulty with measuring cost and benefits of information systems is well documented (Brynjolfsson, 1993). Researchers have more success measuring outcomes measures of success with perceptual measures (i.e., improved communication between managers and users) in contrast to objective measures (i.e. number of security incidents) (Galletta & Lederer, 1989; Premkumar & King, 1994). The use of perceptual measures is also encouraged by Kotulic and Clark (2004) who find research within the information security domain to be challenging and advise against including survey questions asking the respondents to answer sensitive questions (i.e., dollar losses due to security violations or number of security violations) or require the respondent to look up information.

To measure the extent of collaborative exchange in information security planning the respondent is asked to indicate the frequency (range of seldom to almost always) of management, user, and information security manager's participation in information security planning processes. In addition to gathering data on the collaborative exchange within organizations, the survey instrument also assessed the types and number of information security policies in existence within an organization. The National Institute of Standards and Technology Special Publication 800-53 discuss the various types of information security policies. The survey respondents are asked to report yes or no to questions about specific information security policies in use within their respective organization as well answer survey items (range strongly disagree to strongly agree) that address compliance with legal/regulatory requirements and the extent to which the information security function follows documented policies for reporting security violations.

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

Figure 1: Theoretical Model.



Three information security strategies at the organization level are examined using a 5-point likert scale with 1 representing *strongly disagree* and 5 representing *strongly agree*. The recovery measures assess the response capabilities of the information security function and the overall organization to information security incidents. The deterrence measures assess the organization's ability to motivate employees to follow information security policies (Straub & Welke, 1998). Detection measures are designed to assess how the organization identifies incidents of security violations and perpetrators of these violations.

The data was collected by means of a mail survey sent to information security managers, IT managers and high-level executives within an organization. Because the unit of analysis for this study is at the organizational level, a good overall understanding of the information security function within the organization is necessary. In order to measure effectiveness at the organizational level, Seddon et al. (1999) state that top-level management and owners are acceptable query respondents. As a result, the ideal survey respondent is the top-level manager responsible for information security and information systems within an organization. Due to discrepancies in job titles and job differentiation, the survey may not be sent to the appropriate survey candidate. In an attempt to get data from the ideal candidate, the cover letter will ask the individual to forward the survey to the top-level manager directly responsible for the information security function of the organization. Contact information for potential respondents was acquired from Definitive Database, Inc. which has access to subscriber list of many of the information security and IT trade publications.

RESULTS

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

The research design for this study utilizes the survey methodology to assess the relationship between collaborative exchange, formalization of information security activities and effective utilization of information security strategies. The survey instrument was mailed to 1,500 upper-level information security and IT executives requesting their participation. Three months following the initial mailing, a postcard was sent to potential respondents asking them to complete the survey, if they had not already, and return it and also directed the respondent to an on-line version of the survey instrument. A total of 119 useable responses were received resulting in an effective response rate of 12%. To assess the differences between late and early respondents, a t-test of independent samples was conducted on three separate demographic responses showing no significant differences between early and late respondents. A profile of the responding organizations is shown in Tables 1, 2 and 3.

Table 1: Distribution of respondents by type of organization.

	Number of responses	%	Cumulative %
Public	16	13.5	13.5
Private	54	45.4	58.9
Federal	5	4.2	63.1
State	7	5.9	69.0
County	6	5.0	74.0
Municipal	6	5.0	79.0
Educational	14	11.8	90.8
Religious	1	0.8	91.6
Charitable foundation	1	0.8	92.4
Other	9	7.6	100.0
Total	119		

Table 2: Distribution of respondents by industry.

	Number of responses	%	Cumulative %
Construction	2	1.7	1.7
Printing, Publishing	2	1.7	3.4
Transportation	2	1.7	5.1
Consumer Goods Manufacturing	3	2.5	7.6
Capital Goods Manufacturing	2	1.7	9.3
Utilities	1	0.8	10.1
Retail	6	5.0	15.1
Food Service	1	0.8	15.9
Banking, Sec, Invest	12	10.1	26.0
Insurance	4	3.4	29.4
Business Services	7	5.9	35.3
Entertainment	1	0.8	36.1
Health	20	16.8	52.9

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

	Number of responses	%	Cumulative %
Legal	1	0.8	53.7
Education	14	11.8	65.5
Government	20	16.8	82.3
Military	2	1.7	84.0
Other	19	16.0	100.0
Total	119		

Table 3: Distribution of respondents by organization size.

	Number of responses	%	Cumulative %
Less than 500	34	28.6	28.6
500 to less than 1,500	29	24.4	52.9
1,500 to less than 5,000	31	26.1	79.1
5,000 to less than 10,000	9	7.6	86.6
10,000 to less than 50,000	8	6.7	93.3
50,000 or more	8	6.7	100
Total	119		

Table 4 shows the percentage of participating organizations using specific information security policies. Access control policy and procedures is the most prevalent information security policy in use which is understandable as the early beginnings of information security dealt specifically with granting access and separation of duties (Von Solms, 2000). The least used type of information security policy is certification, accreditation and security assessment policy and procedures. Table 5 shows the mean statistics for the line items measuring effective utilization of detection, deterrence, and recovery strategies. All measures show a greater than neutral response except for the line item measuring user training in respect to information security policies. This hints that despite the emphasis placed on user training in information security standards and publications, user training is still a weak point in the information security domain.

Table 4: Distribution of information security policy use.

	Policy Used	%
Access Control Policy and Procedures	114	95.8
Security Awareness and Training Policy and Procedures	96	80.7
Audit and Accountability Policy and Procedures	93	78.2
Certification, Accreditation & Security Assessment Policy and Procedures	48	40.3
Configuration Management Policy and Procedures	89	74.8
Contingency Planning Policy and Procedures	97	81.5
Identification & Authentication Policy and Procedures	104	87.4
Incident Response Policy and Procedures	86	72.3

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

System Maintenance Policy and Procedures	94	79.0
Media Protection Policy and Procedures	92	77.3
Physical and Environmental Protection Policy and Procedures	102	85.7
Security Planning Policy and Procedures	81	68.1
Personnel Security Policy and Procedures	89	74.8
Risk Assessment Policy and Procedures	80	67.2
System and Services Acquisition Policy and Procedures	72	60.5
System and Communication Protection Policy and Procedures	85	71.4
Systems and Information Integrity Policy and Procedures	82	68.9

Table 5: Descriptive Statistics for information security effectiveness.

		Mean	**Std. Deviation**
In the event of an information security violation, the organization has little problem identifying the perpetrator		3.62	0.92
Users caught violating information security policies are disciplined		3.60	1.02
The information security department discovers attacks on the network as they happen		3.51	0.97
Users comply with information security controls		3.42	0.90
Appropriate employees have a good understanding of the organization's disaster recovery plans		3.40	1.06
Users understand the consequences for failure to follow information security policies		3.38	1.02
Appropriate employees have a good understanding of the organization's contingency plans		3.31	1.04
In the event of an information security violation, the organization has little problem identifying how the perpetrator gained access		3.28	0.90
Appropriate employees have a good understanding of the organization's continuity plans		3.22	1.08
Users are sufficiently trained with respect to information security policies		2.95	1.06

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

DATA ANALYSIS

Exploratory factor analysis is one common approach utilized to assess the convergent and discriminant validity of the measurement instruments. Factor analysis is used to assess the dimensionality of survey items which is an assessment of whether multiple items on a measurement instrument measure a single or multidimensional construct. It accomplishes this feat by analyzing the correlations among the various items in the measurement instrument to identify unique factors (Hair et al., 1998).

Sufficient correlations in the data matrix are required for successful application of factor analysis (Hair et al., 1998). Two measures used to assess the appropriateness of the data matrix for factor analysis are the Bartlett test of sphericity and Kaiser-Meyer-Olkin measure of sampling adequacy. The Bartlett test for sphericity assesses the statistical probability of significant correlations among some of the variables (Hair et al., 1998). A significance level less than 0.05 demonstrates acceptable correlations among some of the variables. The measurement instrument show a Bartlett test for sphericity significance level less than 0.01. The Kaiser-Meyer-Olkin measure of sampling adequacy measures the degree of intercorrelations among the variables (Hair et al., 1998). A Kaiser-Meyer-Olkin measure of sampling adequacy of 0.6 or above is acceptable. The performance measurement instruments show Kaiser-Meyer-Olkin measure of sampling adequacy of .799.

Factor analysis was conducted with the criterion of Eigenvalues greater than 1 in order to determine the optimum number of factors. The factor loadings are examined to assess the degree of correlation between the individual variables and the proposed factor structure. Items with a factor loading greater than 0.6 are deemed to be significantly correlated with the proposed factor structure (Hair et al., 1998). While items with factor loading of .3 or more on more than one factor are deemed to be cross-loading across factors and are not unique indicators of a single factor (Hair et al., 1998). Table 6 shows the factor loadings for the performance construct.

After factor analysis, the Cronbach's alpha of each factor is calculated in order to assess reliability. Cronbach's alpha measures the internal consistency of the items in the factor. The lower limit for an acceptable Cronbach's alpha is 0.7 (Hair et al., 1998). The Cronbach's alpha calculations are also shown in Table 6. The total variance explained for the three remaining dependent variables is 73.06%.

Table 6: Factor Analysis Results.

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

	Recovery	Deterrence	Detection
Discover attacks	0.019	0.207	0.695
Identify Perpetrator	0.150	0.009	0.761
How Perp accessed	0.159	0.205	0.831
Understand Consequences	0.183	0.828	0.156
User Comply	0.158	0.848	0.066
Users Disciplined	0.272	0.657	0.249
User Train	0.192	0.734	0.113
Understand Disaster Recovery Plans	0.863	0.227	0.149
Understand Contingency Plans	0.921	0.235	0.137
Understand Continuity Plans	0.913	0.242	0.101
Variance explained	26.44	26.25	19.06
Cronbach's alpha	0.933	0.822	0.692

In addition to factor analysis, the square root of Average Variance Extracted (AVE) for each construct was calculated. AVE is a measure of the percentage of variance that is described by the construct of interest. A comparison of the square root AVE and the correlations of the latent constructs shows proof of discriminant validity (Gefen & Straub, 1997). For proof of discriminant validity, the square root of the AVE must be larger than the correlations. The square root of the AVE for each construct is larger than the respective correlations.

Next is an examination of correlations between the control variables of organization type, size and percent of budget spent on information security. A crosstab and chi-square test of independence between the variables organization size and percentage of budget spent on security (See Table 7) shows no relationship exist between these two control variables. In addition, no relationship is found between organization type and the percentage of budget spent on security (See Table 8).

Table 7: Test of Independence (size versus % of budget spent on security).

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

Cross-tabulation Table				
OBSERVED				
	% of IT budget spent on IT security			
Size	<3%	3% - 7%	>7%	Total
less than 1,500	9	23	29	61
1,500 to less than 10,000	12	18	11	41
10,000 or more	5	7	5	17
Total	26	48	45	119

Calculation of the Chi-Square Test	
DESCRIPTION	VALUE
χ^2*	5.827819
p-value	0.212381
Critical value	9.487729
α	0.05
df	4

Table 8: Test of Independence (org. type versus % of budget spent on security).

Cross-tabulation Table			
OBSERVED			
	% of IT budget spent on IT security		
Organization Type	<3%	>3%	Total
For-Profit	26	43	69
Government	11	12	23
Non-Profit	13	10	23
Total	50	65	115

Calculation of the Chi-Square Test	
DESCRIPTION	VALUE
χ^2*	2.712821
p-value	0.257584
Critical value	5.991465
α	0.05
df	2

Prior to Partial Least Squares (PLS) analysis, regression analysis is performed by regressing number of information security policies, size of organization and percent of security budget on information security effectiveness measures of recovery, detection and deterrence. Tables 9, 10, and 11 show the regression results for number of information security policies and the three effectiveness measures of *recovery, detection,* and *deterrence.* All three regression results show a

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

significant positive relationship between the number of information security policies and the effectiveness of information security measures. An interesting result is seen in regression analysis as percent of budget spent on information security appears to have a significant correlation with recovery measure while it is not significant with detection and deterrence measures. This finding may be due to the observation that deterrence and detection controls are more budget driven and cost are easier to estimate. Meanwhile the expenses of recovery controls are more difficult to estimate and tend to be tied to the number and degree of information security incidents that occur. The organization's ability to effectively recover from security incidents is dependent on having the available resources when needed. Organizations with spend a higher percentage of the budget on information security may have more slack designed for dealing with security incidents as they occur.

Table 9: Information Security Policies and Effectiveness of Recovery Measures.

Variables	β	t-value	p-value
Number of Information Security Policies	0.291	3.180	0.002 ***
Size of Organization	-0.069	-0.867	0.389
% of Budget Spent on Information Security	0.213	3.208	0.002 ***

* $p < 0.10$ ** $p < 0.05$ *** $p < 0.01$

Table 10: Information Security Policies and Effectiveness of Detection Measures.

Variables	β	t-value	p-value
Number of Information Security Policies	0.205	2.899	0.005 ***
Size of Organization	0.002	0.029	0.977
% of Budget Spent on Information Security	0.075	1.473	0.145

* $p < 0.10$ ** $p < 0.05$ *** $p < 0.01$

Table 11: Information Security Policies and Effectiveness of Deterrence Measures.

Variables	β	t-value	p-value

Number of Information Security Policies	0.358	4.941	0.000 ***
Size of Organization	0.052	0.821	0.414
% of IT Budget Spent on Information Security	0.063	1.194	0.236

* $p < 0.10$ ** $p < 0.05$ *** $p < 0.01$

PLS Analysis

This section describes the statistical analysis of the proposed research model and its associated hypothesis using the PLS causal modeling approach. PLS has several advantages over traditional statistical techniques like regression and analysis of variance. PLS has the capability to concurrently test the measurement and structural model and is not constrained to data sets that meet homogeneity and normality requirements (Chin et al., 2003). SmartPLS version 2.0 (Ringle, Wende, & Will, 2005) is used to analyze the measurement model and the structural path between the constructs of interest. In order to obtain reliable results and t-values, 200 random samples of 100 are generated using a bootstrapping procedure. The hypotheses will be evaluated by assessing the sign and significance of the structural path coefficient using one-tailed t-test statistics. PLS Graph does not calculate any goodness-of-fit values, so the coefficient of determination is evaluated to assess the predictive validity of the research model. Figure 2 shows the path coefficients of the PLS model. Table 12 shows the t-values of the PLS model and the results of hypothesis testing.

Figure 2: Results of PLS Analysis.

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

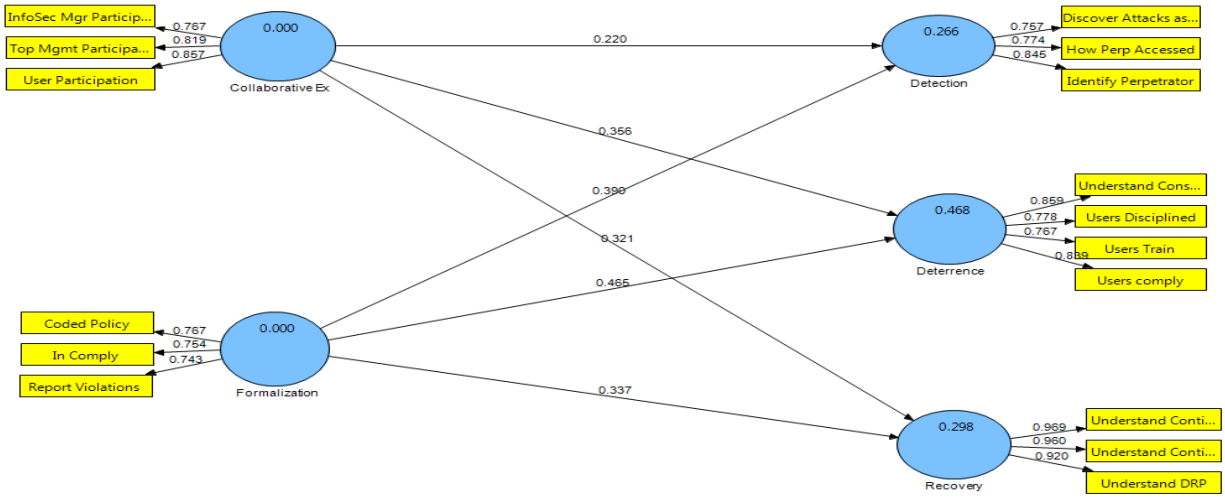


Table 12: Summary of Hypothesis Tests.

Hypothesis	Results	t-value
H_{a1a}: Collaborative exchange will positively impact the effectiveness of information security detection measures.	Supported	2.36*
H_{a1b}: Collaborative exchange will positively impact the effectiveness of information security deterrence measures.	Supported	4.92**
H_{a1c}: Collaborative exchange will positively impact the effectiveness of information security recovery measures.	Supported	3.11**
H_{a2a}: More formalized information security programs are positively associated with higher levels of effectiveness of information security detection measures.	Supported	4.44**
H_{a2b}: More formalized information security programs are positively associated with higher levels of effectiveness of information security deterrence measures.	Supported	6.52**
H_{a2c}: More formalized information security programs are positively associated with higher levels of effectiveness of information security recovery	Supported	3.30**

measures.		

* $p < 0.05$ ** $p < 0.01$

Hypothesis 1a-c proposes that organizations that exhibit higher levels of collaborative exchange when addressing information-security-related concerns and plans will more effectively utilize the information security strategies of detection, deterrence and recovery. The results of hypothesis testing show a positive correlation exist between collaborative exchange and the effectiveness utilization of detection, deterrence and recovery strategies. This result shows the effectiveness of information security within the organization is impacted by the extent of collaborative exchange within the organization. This helps to support past research findings of user and management involvement significantly impacting the performance of specific functions within an organization (Gottschalk, 1999; Sambamurthy et al., 1994; Segars & Grover, 1998) and information security is no exception.

Hypothesis 2a-c proposes that organizations that expend more effort in developing and utilizing information security policies will more effectively utilize the information security strategies of detection, deterrence and recovery. The results of hypothesis testing show a significant positive correlation between extent of information security policy use and the three information security strategies. This finding highlights the value-added associated with establishing specific information security policies within the organization.

To test the predictive power of the PLS model, the explained variance (R^2) is examined for the models of collaborative exchange and formalization on each endogenous construct individually to the full model (Chin, 1998). The PLS models with collaborative exchange and the three constructs of detection, deterrence and recovery explained 13.5%, 28.7% and 20.2% of the variance respectively. The PLS models with formalization and the three constructs of detection, deterrence and recovery explained 22.4%, 36.2% and 21% of the variance respectively. While the PLS model with both collaborative exchange and formalization explained 26.6%, 46.8% and 29.8% of the variance. This increase in explained variance is significant suggesting that the complement of collaborative exchange and formalization together is crucial for effective utilization of detection, deterrence and recovery strategies.

DISCUSSION AND LIMITATIONS

The results of data analysis shows that the degree of formalization of the information security function is correlated with effective utilization of recovery, deterrence, and detection strategies which suggests that organizations are better off creating specific policies to address specific information security concerns within the organization as this may increase user awareness and promote more consistent organizational behavior. However, this study also highlights the importance of developing information security policies while fostering collaborative exchange between the organization's information security function, management and end users of information systems. These results suggest two potential benefits to an organization. First, collaboration between the information security function, management and the end-user, in regards to information security initiatives, may lead to the development of policies that are deemed more relevant to existing threats thereby improving the quality of the formalized policies. Improvements in the quality of the information security policies may lead to better

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

utilization of the available information security strategies to combat existing organizational threats.

Second, end-user involvement in the information security policy development process may lead to higher acceptance and ownership thereby improving the effectiveness of the information security policies and the detection, deterrence and recovery strategies that the policies address. In the end, it is the user who must adhere to the finalized information security policies and attempts to foster collaborative exchange within the organization may advance the user buy-in process. This study shows the importance of the complementary impact of collaborative exchange and formalization on the effectiveness of the information security function and discredits the notion that information security policies is best developed by the information security function and/or upper-level management and then circulated to the end user for compliance. The danger inherent is leaving the decision-making involved in the policy development process to the information security function or management alone may lead to user resistance and less compliance. Fostering an environment of free exchange of ideas within the organization with regards to information security initiatives offers the user a glimpse into the threats facing the organization thereby increasing the perceived importance of implementing and complying with information security policies.

There are several limitations inherent in this study. First limitation is common method variance as information from one respondent within each organization was gathered. Another limitation is this study's cross sectional design only permits claims of correlation not causation. One last limitation is desirability bias reporting. Social desirability bias is present when respondents overrate positive survey questions and underrate negative survey questions. As the survey instrument was sent to respondents with information security responsibility within their respective organizations, this bias may be present.

REFERENCES

Adria, M., & Chowdhury, S. D. (2004). Centralization as a design consideration for the management of call centers. *Information and Management*, 41(4), 497-507.

Bidgoli, H. (2003). An integrated model for improving security management in the e-commerce environment. *Journal of International Technology and Information Management*, 12(2), 119-134.

Blakley, B, McDermott, E., & Geer, D. (1991). Information security is information risk management. *Proceedings of the 2001 workshop on New Security Paradigms* (97-104).

Bodin, L. D., Gordon, L. A., & Loeb, M. P. (2005). Evaluating information security investments using the analytic hierarchy process. *Communications of the ACM*, 48(2), 79-83.

Brancheau, J. C., Schuster, L., & March, S. T. (1989). Building and implementing an information architecture. *Database*, 19(2), 9-17.

  ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

Brynjolfsson, E. (1993). The productivity paradox of information technology. *Communications of the ACM* , 36(12), 67-77.

Byrd, T. A., Sambamurthy, V., & Zmud, R. W. (1995). An examination of IT planning in a large, diversified public organization. *Decision Sciences*, 26(1), 49-73.

Chang, S. E., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*, 106(3), 345-361.

Chi, l., Jones, K. G., Lederer, A. L., Li, P., Newkirk, H. E., & Sethi, V. (2005). Environmental assessment in strategic information systems planning. *International Journal of Information Management*, (25), 253-269.

Chin, W. W. (1998). Issues and opinions on Structural Equation Modeling. *MIS Quarterly*, 22(1), vii – xvi.

Chin, W. W., Marcolin, B. L., & Newsted, P. R. (2003). A partial least squares latent variable modeling approach for measuring interaction effects: Results from a monte carlo simulation study and an electronic-mail emotion / adoption study. *Information Systems Research*, 14(2), 189-217.

Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review*, 45(1), 67-87.

Galletta, D. F., & Lederer, A. L. (1989). Some cautions on the measurement of user information satisfaction. *Decision Sciences* 20(3), 419-438.

Garrison, C. P., & Posey, R. (2006). Computer security checklist for non-security technology professionals. *Journal of International Technology and Information Management*, 15(3), 87-91.

Gefen, D., & Straub, D. (1997). Gender difference in the perception and use of e-mail: an extension to the technology acceptance model. *MIS Quarterly*, 21(4), 389-400.

Gottschalk, P. (1999). Implementation predictors of strategic information systems plans. *Information and Management*, 36(2), 77-91.

Hair, J. F., Anderson, R. E., Tatham, R. L., & Black, W. C. (1998). *Multivariate Data Analysis with Readings* (5th ed.), Englewood Cliffs, NJ, Prentice Hall.

Hartono, E., Lederer, A. L., Sethi, V., & Youlong, Z. (2003). Key predictors of the implementation of strategic information system plans. *Database for Advance in Information Systems*, 34(3), 41-53.

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

James, H. L. (1996) Managing information systems security: a soft approach. *Proceedings of the Information Systems Conference of New Zealand* (pp. 10-20).

Jansen, J. J. P., Van Den Bosch, F. A. J., & Volberda, H. W. (2006). Exploratory innovation, exploitative innovation, and performance: effects of organization antecedents and environmental moderators. *Management Science,* 52(11), 1661-1674.

Jitpaiboon, T., & Kalaian, S. A. (2005). Analyzing the effect of top management support on information systems performance across organizations and industries using hierarchical linear modeling. *Journal of International Technology and Information Management*, 14(2), 131-144.

Kankanhalli, A., Teo, H., Tan, B. C. Y., & Wei, K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, 23, 139-154.

King, W. R., & Kraemer, K. L. (1984). Evolution and organizational information systems: An assessment of Nolan's Stage Model. *Communications of the ACM*, 27(5), 466-475.

Kotulic, A., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information and Management*, 41(5), 597-607.

Lederer, A. L., & Mendelow, A. L. (1987). Information resource planning: Overcoming difficulties in identifying top management's objectives. *MIS Quarterly*, 11(3), 389-399.

Lederer, A. L., & Salmela, H. (1996). Toward a theory of strategic information systems planning. *Journal of Strategic Information Systems*, 5, 237-253.

Lederer, A. L., & Sethi, V. (1992). Root causes of strategic information system planning implementation problems. *Journal of Management Information Systems*, 9(1), 25-46.

Pattinson, M. R., & Anderson, G. (2007). How well are information risks being communicated to your computer end-users? *Information Management and Computer Security*, 15(5), 362-371.

Premkumar, G., & King, W. R. (1994). Organizational characteristics and information system planning: An empirical study. *Information Systems Research*, 5(2), 75-109.

Sabherwal, R. (1999). The relationship between information system planning sophistication and information system success: An empirical assessment. *Decision* Sciences, 30(1), 137-167.

Sambamurthy, V., Zmud, R. W., & Byrd, T. A. (1994). The comprehensiveness of IT planning processes: a contingency approach. *Journal of Information Technology* Management, 5(1), 1-10.

Sasidharan, S., Wu, J., Pearce, D., Kearns, G. S., & Lederer, A. L. (2006). The role of convergence in information systems and business planning. *Journal of International Technology and Information Management*, 15(3), 1-18.

Schultz, E. E., Proctor, R. W., Lien, M. C., & Salvendy, G. (2001). Usability and security – An appraisal of usability issues in information security methods. *Computers & Security*, 20(7), 620-634.

Seddon, P. B., Staples, S., Patnayakuni, R., & Bowtell, M. (1999). Dimensions of information systems success. *Communications of the Association of Information Systems*, 2(20), 2-60.

Segars, A. H., & Grover, V. (1998). Strategic information systems planning success: An investigation of the construct and its measurement. *MIS Quarterly*, 22(2), 139-163.

Stanton, J. M., Guzman, I., Stam, K. R., & Caldera, C. (2003). Examining the linkage between organizational commitment and information security. *International Conference Systems, Man and Cybernetics*, 3, 2501-2506.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, 22(4), 441-469.

Teo, T. S. H., & Ang, J. S. K. (2001). An examination of major IS planning problems. *International Journal of Information Management*, 21, 457-470.

Von Solms, B. (2000). Information security – The third wave. *Computers & Security*, 19(7), 615-620.

Wade, J. (2004). The weak link in IT security. *Risk* Management, 51(7), 32-37.

Zmud, R. W. (1982). Diffusion of modern software practices: Influence of centralization and formalization. *Management Science,* 28(12), 1421-1431.

Zollo, M. M., & Winter, S. G. (2002). Deliberate learning and the evolution of dynamic capabilities. *Organization Science*, 13, 339-351.

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

This Page Left Intentionally Blank

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy