Communications of the Association for Information Systems

Volume 26 Article 13

3-2010

Empirical Evaluation of Information Security Planning and Integration

Randall F. Young
University of Texas–Pan American, YoungRF@utpa.edu

John Windsor
University of North Texas

Recommended Citation
Young, Randall F. and Windsor, John (2010) "Empirical Evaluation of Information Security Planning and Integration," *Communications of the Association for Information Systems*: Vol. 26 , Article 13.
DOI: 10.17705/1CAIS.02613
Available at: https://aisel.aisnet.org/cais/vol26/iss1/13

Communications of the Association for Information Systems

CAIS

Empirical Evaluation of Information Security Planning and Integration

Randall F. Young

University of Texas–Pan American

YoungRF@utpa.edu

John Windsor

University of North Texas

Abstract:

Organizations can choose how to integrate information security through planning and structuring of the information security function. This study aims to examine how the planning and structuring choices of the organization impacts the effective utilization of information security strategies. This study examines information security planning integration through a stages of growth perspective and finds that more mature information security planning integration is positively correlated with more effective utilization of information security deterrence, detection, and recovery strategies. This study also finds that a decentralized structure of information security management activities has a positive effect on the maturity of information security planning integration. This study suggest the maturity of information security planning integration that has a direct effect on the utilization of information security strategies and mediates the relationship between structure of information security management activities and utilization of information security strategies.

Keywords: Information security planning, information security integration, information security strategies, stages of growth

Volume 26, Article 13, pp. 245-266, March 2010

The manuscript was received 3/25/2009 and was with the authors 5 months for 1 revision.

I. INTRODUCTION

A recent survey found that, as far as management is concerned, information security was not among the top ten critical issues in management of information systems [Pimchangthong et al. 2003]. However, there are indications that management's perceptions about information security may be changing. New laws, like the 2002 Sarbanes-Oxley Act, are increasing management's liability with respect to protecting financial information under their control, and evidence suggests information security breaches are problematic in many organizations. According to the 2007 Computer Security Institute/Federal Bureau of Investigation Computer Crime and Security Survey, 46 percent of organizations surveyed experienced a financial loss due to a security breach, with a total loss estimate of $67 million.

The discipline of information security management is still in its infancy, as evidenced by the lack of empirical scholarly work in this area. The little empirical research that has been conducted has shown that poor information security management practices exist within many organizations [Baskerville 1993; Kankanhalli et al 2003; Shimeall and McDermott 1999]. Most research on information security focuses on specific technologies and algorithms and how it impacts the principles of confidentiality, integrity, and availability. But an important area receiving little attention is the antecedents of effective information security management at the organizational level [Stanton et al 2003].

One of the aims of this study is to identify the stages of growth with respect to information security planning. This research study will apply King and Teo's [1997] four-stage evolutionary model of business/information system planning integration to information security planning in organizations. The benefits of this are twofold: (1) currently there is little understanding of how growth of information security capabilities is taking place, and (2) there is a plethora of frameworks for the information security discipline but no obvious ties between them. This stage model will provide a new conceptual lens by which information security can be observed, analyzed, and managed. Identifying a stage model can assist management with the orderly transition among the stages [Drury 1983], as well as identify the current attitudes, management practices, and integration of information security within the organization. Another aim of this study is to empirically examine the influence of information security planning integration in explaining variation in the effective use of information security strategies. Lastly, the issues of centralization versus decentralization of information security planning activities will be evaluated along with its impact on the stages of information security planning integration and effective utilization of information security strategies.

This study makes several contributions to the information security discipline. First, this study provides a different perspective of evaluating the effectiveness of the organization's information security function. In addition, the stages of information security approach gives analysts and organization executives a means to assess whether conditions in place are facilitating or obstructing future growth of the information security function. A final contribution is evaluating how organization's choices in regards to the structure of the information security activities impact information security planning integration and the effective utilization of information security strategies. The rest of this paper is organized into four sections. The first section describes past research and the development of our model along with the related hypotheses. The second section describes the research methodology followed by a discussion of the data results. The third section describes the statistical analysis of the proposed model. The last section presents the conclusions of our research along with limitations and directions for future research.

II. LITERATURE REVIEW

The rationale behind the use of the literature on information systems planning in this study is twofold. First, Nolan [1973], in his original description of the stage hypothesis, states that stages can be identified through measurement of the central tendencies that appear in the nature of planning, organizing and controlling tasks associated with the computer resource. As the critical nature of systems grow in importance and the complexity of systems increase, planning becomes one of the chief mechanisms employed by organizations to reduce uncertainty, ensure the availability of staff, hardware, software and financial resources and improve effectiveness [McFarlan et al.,1983]. Second, the purpose of information systems planning changes as information systems technology evolves [McFarlan et al. 1983; Pyburn 1983]. Therefore, as organizations become more mature in the domain of information security, the planning, control, and management techniques must evolve as well, and this is one method by which to identify stages.

Stages of Growth

Many researchers who examine the corporate lifecycle from birth and ultimately to decline predict that variables among environment, strategy, structure, and decision-making methods are significantly different in each stage [Miller and Friesen 1984]. Nolan [1973], borrowing from these lifecycle theorists, made the assertion that the computer budget is a suitable surrogate by which to measure changes in an organization's environment, strategy, uses of computer technology, and planning and control tasks. As a result, an organization's computer budget will give some indication about the stages-of-growth phenomena within the information systems domain [Benbasat et al. 1984; King and Kraemer 1984]. However, several studies failed to empirically validate this assertion [Lucas Jr. and Sutton 1977; Drury 1983]. Nolan [1973] would also go on to theorize that with each successive stage the objectives of the computer resource, and the organizational responsibility and authority of the computer resource function will shift. He would speculate that, as the information system organization matured, the skills of the information system managers would shift from a heavy technical focus to a more managerial and administrative focus [Nolan 1973].

In 1979, Nolan [1979] proposed a set of benchmarks to measure the stages of growth of the data processing function, which included expenditures, technology, applications portfolio, information system organization, information systems planning and control, and user awareness. Empirical support for the benchmarks of computer budget, the applications portfolio, and data administration have not materialized, while other benchmarks have found either strong or partial empirical support [Benbasat et al. 1984]. Since Nolan's [1973, 1979] work, the stage hypothesis approach has been adapted to evaluate end-user computing [Huff et al. 1988], business planning and IS planning integration [King and Teo 1997], information centers [Magal et al. 1988], and end-user satisfaction [Mahmood and Becker 1985–1986].

One of the drawbacks to the stage hypothesis concept is lack of empirical support. Several studies have attempted to empirically validate the stages of growth with little success [Drury 1983; Huff et al. 1988]. Two manuscripts authored by King and Kraemer [1984] and Benbasat et al. [1984] found a number of problems in Nolan's method of identifying the stages of computing growth. For instance, King and Kraemer [1984] challenged some of Nolan's assumptions like the assertion that the computer budget is a useful surrogate for growth and the contention that technological change is the trigger driving change. But despite these limitations, researchers are continuing to refine and adapt the stage hypothesis model and analyze it in different contexts within the IS discipline. One explanation for the lack of empirical support is the difficulty of accurately measuring the underlying changes in environment, structure, strategy, planning and control [Benbasat et al. 1980]. Research in organizational lifecycle and some more recent research in information systems addressing the stage hypothesis have found some interesting correlations and patterns that suggest the stage-of-growth phenomena is evident with proper measurement and analysis techniques [Miller and Friesen 1984; King and Teo 1997; Huff et al. 1988].

Information Security Planning Integration Benchmarks

Role of Information Security Management

A critical factor impacting the effectiveness of an organizational function is the agreement or lack thereof between senior management and the function concerning roles [Lederer and Salmela 1996; Riech and Benbasat 1996; Magal et al. 1988]. As such, research examining the role of organizational functions must assess the perspective of both the function and senior management [Boynton et al. 1994]. Any inconsistency in understanding of roles can impact the effectiveness of the information security function. In addition, through the identification of the role of different functions, we can characterize the position of the functional units within an organization [McFarlan et al. 1983].

The responsibility of the information security manager has expanded from the protection of information within the organization to the need to protect information in an extended enterprise [Fried 1994; Da Veiga and Eloff 2007]. In addition, the information security manager must work with service providers and ensure that continuity-of-operation plans of critical services are adequate [Dutta and McCrohan 2002]. The decentralization of data and data processing and increasing interconnectivity between organizations and customers is, again, promoting a change of the information security officer's role in the organization [Dhillon and Backhouse 2000]. Control becomes increasingly difficult in this environment. The role of the information security officer will turn to educating employees so that they can make the appropriate decisions in any situation they may encounter [Dhillon and Backhouse 2000].

Top Management and User Participation

Research suggests that user and management expectations influence success [Cheney et al. 1986; Dearden 1972]. Two methods useful for managing management and user expectations are training and inviting user and management involvement in the development and planning process. The importance of top management support of the planning process has been well established in the literature [Lederer and Salmela 1996; Byrd et al. 1995; Earl 1993; Hartono et al. 2003]. In addition, many studies have found that top management involvement is crucial to the success of information system planning [Lederer and Sethi 1988; Premkumar and King 1994]. Involvement goes

beyond support in that it includes top management's time and knowledge inputs, not just monetary support and a slap on the back. The involvement of top management is necessary for the information security planning process to promote an organization planning approach. Planning with a top-down focus, broad participation, and preset planning cycles increases the ability of planning teams to align strategies and plans within the organization [Brown 2004]. A high degree of alignment between information system plans and business plans has been shown to lead to a high level of management commitment to the information system plans [Lederer and Salmela 1996], more of the plan being implemented [Gottschalk 1999], and increase visibility of the information security function [Lederer and Sethi 1996].

One of the first critical steps in the information security planning process is acquiring top management support. It is through top management support that recognition of the importance of information security planning is communicated throughout the organization. The information security planning process will be ineffective in an environment where top management has a low level of ownership of the information security philosophy [Atkinson 2005; Earl 1993]. A low level of attention from management will result in a low level of concern among employees [Thong et al. 1996]. Byrd et al. [1995] find a significant positive relationship between top management support and the resultant quality of the plans. They also find that the larger the firm the more significant the relationship between top management support and plan quality.

Going beyond top management support, many researchers recognize that top management involvement of high quality is critical to the success of information system planning projects [Lederer and Sethi 1991; Premkumar and King 1994]. The inputs of top management will influence the alternative futures identified and evaluated during the planning process [Lederer and Mendelow 1987]. In addition, top management support and active involvement will facilitate management buy-in which will be necessary for plan implementation to happen. In fact, Teo and Ang [2001] find "difficulty to secure top management commitment to implement the IS plan" and "ignoring the IS plan once it has been developed" to be two of the top problems facing information system planners. This difficulty with getting management to support implementation may be due, in large part, to the actual plan being inconsistent with top management's expectations [Lederer and Sethi 1991]. Through active management involvement, information security planners can develop plans more in line with managements' expectations, which will reduce wasted effort, time, and expense.

Numerous studies promote the importance of getting users involved in the planning and implementation process [Lederer and Sethi 1991; Segars and Grover 1998; Peffers et al. 2003]. The benefits, touted in the literature, of active user involvement, include higher user acceptance, awareness, and ownership [James 1996], greater extent of plan implementation [Gottschalk 1999], and higher quality input for the planning process [Lederer and Mendelow 1987]. Ultimately it is the users who must abide by and use the prescriptions that make up the finalized information security plan. The users have been consistently viewed as the weak link in the information security literature [Schultz et al. 2001; Wade 2004; Von Solms 2000]. 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. An environment of discord is at odds with the ideals of a collaborative, knowledge-sharing organization.

The notion of user acceptance and its impact on behavior and IT use has spawned several well-studied theories and models like the Technology Acceptance Model, the Theory of Reasoned Action, and the Theory of Planned Behavior [DeLone and McLean 2003; Venkatesh et al. 2003]. In the information system planning literature, user acceptance has been found to be critical to the implementation of final plans [Gottschalk 1999]. Failure to implement final plans is one of the top problems facing information system planners [Hartono et al. 2003], and without implementation the information security planning process is wasted. One of the most effective ways to get users to accept plans is by getting the users involved in the planning process [Peffers et al. 2003]. Users are more accepting of information security measures when they are involved in the process and contributed to the solution [James 1996; Pattinson and Anderson 2007].

The knowledge of the vulnerabilities, threats, and risk that face an organization are not exclusively or conclusively known at the executive level or within the information security function [James 1996; Pattinson and Anderson 2007]. An effective information security process entails scanning the internal and external environment for threats, vulnerabilities, and probabilities of occurrence [Loch et al. 1992]. Through widespread user participation, good quality information can be contributed to the planning process leading to better plans [Peffers et al. 2003]. In addition, within the information security alternatives, there may be usability issues that will impact user resistance and the participation of users can help to identify these issues [Chang and Chin-Shien 2007; Schultz et al. 2001].Organizations shown to effectively use organizational resources to achieve information security and control objectives are characterized as having a strong management support and leadership team that embraces user involvement in the planning phase [ISACA 2009; Pattinson and Anderson 2007].

Triggers of Information Security Investment and Performance Structure

The factors, identified in the literature, that trigger information security investment and evaluation include discovered information security abuses [Hoffer and Straub 1989], government legislation, media reports, and pressures from clients and business partners [Kwok and Longley 1999]. Cavusoglu et al. [2004] identify four approaches an organization may use to make information security investment decisions that utilize fear and uncertainty, budget restrictions, proxy variables or risk analysis. Traditional approaches to information security assessment utilize highly structured methods to evaluate systems. These methods include audit/checklist methods, risk analysis/risk assessment methods, and cost accounting/cost justification methods. For instance, the Information Systems Audit and Control Association (ISACA) published a detailed audit checklist aimed to assess IT governance issues, which includes information security. The Government Accountability Office publishes a risk assessment methodology that looks at risk to monetary loss, risk to productivity loss, and risk to loss of customer confidence due to a variety of information security violations. And the National Institute of Standards and Technology (NIST) Special Publication 800–30 directs information security managers on how to conduct a risk analysis. The NIST also publishes another special publication (SP 800–55) that offers a list of information security metrics that organizations may use.

There are several major criticisms of these highly structured methods; one is the lack of attention directed to people considerations [James 1996; Dhillon and Backhouse 2001]. Another criticism is the narrow focus of information security that these methods promote [James 1996] and yet another criticism aimed specifically at risk analysis is that the process tends to raise more questions than answers [Kwok and Longley 1999; Parker 2007]. It is very difficult to measure information security, and, without convincing information security performance measures, the information security officer may find budget justification to be difficult [Bodin et al. 2005; Kwok and Longley 1999].

Status of Information Security Function

McFarlan et al. [1983] finds the role of information systems in the organization's operations or strategy impacts the status level of the information systems manager. Within organizations, the information systems security management position has evolved in the form of job responsibility and authority [Wylder 1992]. This evolution is a result of the changes that occur in organizations in reaction to a changing environment and increasing importance of the information security function [Wylder 1992]. The status and level of authority granted to the information security officer has been found to significantly influence the success of the information system planning process [Pyburn 1983]. The results of the information security function and the information security executive getting closer to top management is a more effective information security planning process. In fact, Lederer and Sethi [1988] find that when the information system executive reported to an organizational level responsible for operational issues (such as a controller), they experienced more critical problems in comparison to organizations where the information system executive reported to a higher level. Kwok and Longley [1999] list five common problems faced by information security officers with inadequate status with the organization which includes lack of full commitment from senior management, difficulty in deciding how much security is required and difficulty convincing current levels of security to auditors.

Information Security Manager Involvement in Business Planning

Top management involvement in the information security planning process has been found to increase information system planning success [Lederer and Sethi 1988; Premkumar and King 1994]. The participation of information system executives in the business planning process has also been shown to lead to increased information system planning success [Lederer and Sethi 1992]. In order to produce useful, relevant information security plans, the information security officer must understand the objectives and strategies of the firm in order to produce information security plans that fit the organization. Pyburn [1983] suggests that many organizations fail to communicate and document completely the strategies and plans of the organization. When strategy decisions and plans are documented, it is common to find that the documents are severely lacking in details and subsequently fail to adequately guide the information system planners [Henderson and Sifonis 1988]. When information security is viewed as having a strategic impact on the organization, the information security executives being left out of the communication loop likely renders the information security function ineffective. Some of the benefits that arise from the information system executive's participation in the business planning process include better information systems planning and better utilization of resources [Sabherwal 1999].

Participation in the organizational planning process also gives the information security executive the occasion to educate top management about potential information security issues [Premkumar and King 1994]. In addition, the participation of top information system executives in the business planning process has also been shown to lead to increased support of information system plan implementation [Lederer and Sethi 1992]. If the information security plans do not address the organizational goals and strategies, top management will view the plan as lacking in relevance and view the information security executive as unknowledgeable about the business issues facing the organization [Lederer and Sethi 1992]. The first three hypotheses of interest are:

H_{a1a}: More advanced stages of information security planning integration are associated with higher levels of effectiveness of information security recovery measures.

H_{a1b}: More advanced stages of information security planning integration are associated with higher levels of effectiveness of information security deterrence measures.

H_{a1c}: More advanced stages of information security planning integration are associated with higher levels of effectiveness of information security detection measures.

IT Organizational Structure

The belief that organization and IT structure are factors impacting the success, or lack thereof, of the information systems function is driving past and current research [Adrai and Chowdhury 2004]. Success has been shown to be partially impacted by the management level that is responsible for the MIS function [Alloway and Quillard 1983; Ein-Dor and Segev 1982]. For this study, the focus will be exclusively on the centralization/decentralization of information security management activities. The range of prior academic research within the information systems domain that has focused on structure from a centralization/decentralization perspective include examining the impact of structure on innovation [Moch and Morse 1977; Zmud 1982], information services [Olson and Chervany 1980, MIS structure [Ein-Dor and Segev 1982], management of call centers [Adria and Chowdhury 2004], quality of computing service [Danziger et al. 1993], and organizational competitive strategy [Tavakolian 1989].

The centralization/decentralization decision is a difficult one for management, as evident by the constant tinkering and movement between the two extremes [Ein-Dor and Segev 1978; King and Kraemer 1984]. The decision to centralize or decentralize information system resources presents unique technical and organizational challenges that impact the effectiveness of providing information services [Adria and Chowdhury 2004]. Despite these technical and organizational concerns, political and bureaucratic influences are major factors impacting the centralization/ decentralization decisions [George and King 1991; King 1983].

The information security resources can be centralized, shared between central authority and user groups, or decentralized [Kotulic and Clark 2004]. It has been suggested that centralization is more effective preventing information security violations through organization-wide establishment of policies and better monitoring [Kotulic and Clark 2004]. However, it has also been suggested that, as organizations become more sophisticated and the environment becomes more uncertain, the ability to manage in a centralized manner becomes more difficult [Benjamin et al. 1985; Govindarajan 1986]. So, in response to greater sophistication and uncertainty, some of the decision-making authority must be reassigned to divisions and departments. However, when lower-level employees are incompetent to handle certain decisions, the decentralization choice is perilous at best [Nault 1998]. An important caveat in the design of the structure of the information security function is specific recognition of decision authority and no sharing of decision rights. This leads us to our next hypothesis:

H_2: More advanced stages of information security planning integration are positively associated with more centralized information security management activities.

Prior research attempting to link organizational structure and outcome measures have resulted in conflicting findings due to environment, strategy, and technology factors [Fry 1982]. As a result, the information security planning integration is believed to account for a significant amount of the variance in the dependent variable. With the addition of the mediator variable, the independent variable (information security management structure) is assumed to have a small or non-significant effect on the dependent variable. However, it is believed that conditions in the information security management structure may enable or obstruct the organization's ability to effectively reach certain stages of advanced information security planning integration and, therefore, is an important construct in the model. This leads to the final hypotheses of interest below:

H_{a3a}: Information security planning integration will mediate the impact of information security management activities on the effectiveness variables of information security recovery measures.

H_{a3b}: Information security planning integration will mediate the impact of information security management activities on the effectiveness variables of information security deterrence measures.

H_{a3c}: Information security planning integration will mediate the impact of information security management activities on the effectiveness variables of information security detection measures.

III. METHODOLOGY

This research model, as seen in Figure 1, encompasses five constructs: the information security structure, information security planning integration, information security recovery strategies, information security deterrence strategies and information security detection strategies.

Research Instrument

Following the template used by Zmud [1982], the survey items request the location of responsibility for each major organization-wide information-security decision task. The location of responsibility includes board of directors or steering committees, chief executive officer (CEO), chief information security officer (CISO), information security officer (ISO) or chief information officer (CIO), divisional or functional manager, sub-department managers, and lower-level information security personnel/analyst. The location of responsibility for each activity will be coded as 1 being the highly centralized position (owners/board of directors) through 6 which represents the most decentralized position (lower-level information security personnel/analyst).

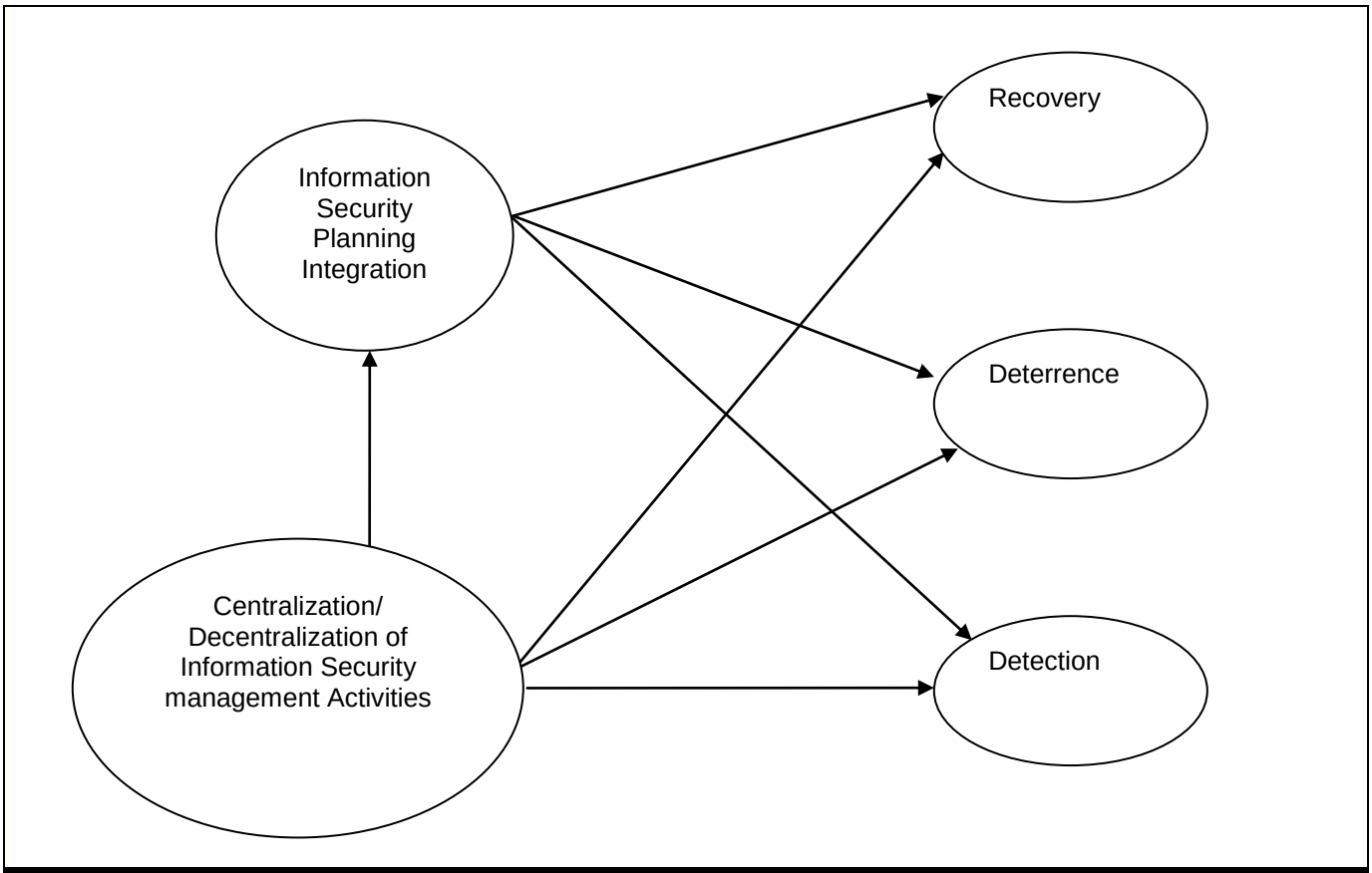

Figure 1: Research Model.

The survey items to operationalize this information security planning integration construct are pulled from King and Teo's [1997] manuscript on IT-business planning integration and an analysis of the literature in the information security domain. The measurement instrument for the organization's information security planning integration encompasses eight benchmarks that assess alignment of information security with business objectives and interaction among stakeholders within the organization. The measurement instrument will ask the respondents to choose one of four descriptions within each benchmark that most represents their organization.

Premkumar and King [1994] suggests that researchers have more success measuring outcome variables of planning, strategy, and structure decisions through the use of perceptual measures (i.e., improved communication between managers and users) in comparison to more objective measures (i.e., number of security incidents, financial costs of security incidents, etc.). Due to the well-documented problems with measuring cost and benefits of information systems [Brynjolfsson 1993], perceptual measures are prominent in effectiveness, success, and performance research [Galletta and Lederer 1989]. In addition, the use of perceptual measures is encouraged by Kotulic and Clark [2004] who find research within the information security domain to be difficult and discourage

survey questions that ask respondents to answer sensitive questions (i.e., dollar losses due to security violations or number of security violations) or questions that require the respondent to look up information.

For this study, three information security strategies at the organization are examined. The perceived effective use of these three information security strategies will be measured through a 5-point likert scale with 1 representing *strongly disagree* and 5 representing *strongly agree*. The recovery measures are designed to assess the response capabilities of the information security function and the overall organization to information security incidents. The deterrence measures are designed to assess the organization's ability to motivate employees to follow information security policies [Straub and Welke 1998]. Detection measures are designed to identify potential information security violations and the perpetrators of such violations.

Baron and Kenny [1986] propose two methods of evaluating a model that includes a mediating variable: three-step regression and structural equation modeling. However, some researchers question the use of SEM in an exploratory mode [Chin 1998; Lee et al. 1997]. Chin [1998] suggest use of the Partial Least Squares (PLS) statistical approach for research studies where the underlying models are still in the early stages of development. As the research model of interest in this study is a new and untested model, the PLS technique will be used to explore the relationships between the measurement model and the structural model.

PLS is a components-based structural equation modeling technique used to analyze research models that contain unobservable latent variables [Gopal et al. 1992–1993]. A strength of the PLS statistical technique lies in its ability to simultaneously model the structural paths and the measurement path with small to medium sample sizes [Chin et al. 2003]. The measurement model encompasses the relationship between the directly observable survey items and the unobservable constructs (latent variables). The structural model represents the proposed relationship between the latent variables. One alternative method of assessing the structural model is through regression analysis. While this and other multivariate techniques break up the assessment of the measurement and structural model, PLS evaluates both concurrently.

IV. RESULTS

The data was collected by means of a mail survey sent to information security managers, IT managers, and high-level executives within an organization. See Table 1 for a profile of respondents. 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. Of the 1500 surveys mailed out, a total of 180 were returned. Of the 180 surveys returned, 61 were discarded because the contact person was no longer employed by the organization. Extrapolating the 61 unusable responses out of the 180 total surveys to the population suggests that 508 out of the 1500 contacts surveyed may be incorrect contact addresses. A total of 116 responses was received from the initial mail out. A follow-up mailing, to improve the response rate, was sent after three months and requested their participation by directing the respondent to an on-line version of the survey instrument. The second mailing resulted in an additional 64 responses. Using the remaining 992 as the total population, the 119 useable responses results in a response rate of 12 percent. Non-response bias attempts to identify characteristics that may differ between respondents and non-respondents. To assess the differences between late and early respondents, a t-test of independent samples was conducted on three separate demographic responses. All p-values are greater than .10, showing no significant differences between early and late respondents.

A varied cross-section of organizations and industries are represented in the data set. For profit companies represent the bulk of the respondents (58.83 percent). Government organizations represent 21.84 percent, and not-for-profit organizations represent 19.32 percent of the data set. While there are a variety of industries represented in the data set, more than half of the respondents classify themselves as financial, healthcare, education or government, as seen in Table 2. The majority of the organizations participating in the survey employ less than 5,000 employees (79.1 percent), as seen in Table 3.

Table 1: Profile of Respondents			
	Number of responses	%	Cumulative %
CIO	42	35.29	35.29
CISO	8	6.72	42.01
ISO	6	5.04	47.05
CTO	3	2.52	49.57
Director of IT	23	19.33	68.9
Director of IT Security	2	1.68	70.58
VP of IT/Information Services	11	9.24	79.82
Manager of IT	5	4.2	84.02
Manager of Information Security	9	7.56	91.58
Security Analyst	4	3.36	94.94
Asst Comptroller	1	0.84	95.78
Info Security & Network Administrator	3	2.52	98.3
Software Engineer	1	0.84	99.14
Missing value	1	0.84	99.98
Total	119		

Table 2: Industry of Respondent's Organization			
	Number of responses	%	Cumulative %
Agriculture	0	0	0
Mining	0	0	0
Construction	2	1.68	1.68
Printing, Publishing	2	1.68	3.36
Transportation	2	1.68	5.04
Consumer Goods Manufacturing	3	2.52	7.56
Capital Goods Manufacturing	2	1.68	9.24
Utilities	1	0.84	10.08
Retail	6	5.04	15.12
Food Service	1	0.84	15.96
Banking, Sec, Invest	12	10.08	26.04
Insurance	4	3.36	29.4
Real Estate	0	0	29.4
Hotels	0	0	29.4
Business Services	7	5.88	35.28
Entertainment	1	0.84	36.12
Health	20	16.81	52.93
Legal	1	0.84	53.77
Education	14	11.76	65.53
Government	20	16.81	82.34
Military	2	1.68	84.02
Telecommunications	0	0	84.02
Other	19	15.97	99.99
Total	119		

Table 3: Size of Respondent's Organizations			
	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		

Most organizations have an idea of how much of their IT budget is spent specifically on security as shown in Table 4. However, nine respondents answered *unknown* to the question asking about percentage of IT budget spent on security. This does not imply these organizations are failing to implement security in the IT organization. Two organizations commented that their security and IT budget was intertwined as security is being designed into all IT projects, making it difficult to separate non-security related activities from security related activities. This is not an unexpected result, as it is widely accepted that the most effective way to secure systems is by designing security into the system during the initial stages of the system development lifecycle. A crosstab and chi-square test of independence shows no significant relationship exists between the variables organization size and percentage of IT budget spent on IT security ($\chi^2 = 5.83$; p-value = 0.21). A crosstab and chi-square test of independence also shows that no significant relationship exists between the variables organization type (for-profit organizations, government organization, or non-profit organizations) and percentage of IT budget spent on IT security ($\chi^2 = 2.71$; p-value = 0.26).

Table 4: Distribution of Respondents by Portion of IT Budget Spent on Security			
	Number of responses	%	Cumulative %
Less than 1%	19	16.0	16.0
1% to 2%	22	18.5	34.5
3% to 5%	39	32.8	67.3
6% to 7%	9	7.6	74.9
8% to 10%	14	11.8	86.7
More than 10%	3	2.5	89.2
Unknown	9	7.6	96.8
Missing values	4	3.4	100.2

The results from the survey examining the effectiveness of information security practices shows that the average response was 3.4584. As the survey instruments utilizes a 5-point likert scale, this average implies a better than neutral response to effective information security practices. An interesting result of this instrument is the two information security practices with a lower-than-neutral response concerning user training. Despite numerous publications highlighting the critical importance of adequate user training, user training is still perceived to be a weak area in many organizations, and this may very well explain the next finding discussed. The effectiveness measure with the highest response concerns the ability of the information security department to quickly implement corrective measures in response to an information security breach. Poor user training may be leading to a large number of easily avoidable information security breaches forcing the information security department to come in and save the day. Due to plenty of practice, the strength of the information security department may not be in preventing information security breaches but helping the organization recover from information security breaches.

The information security planning integration measurement instrument asks respondents to review four choices for each benchmark and choose the response most representative of their organization. Each choice is tied to one of four levels of information security planning integration maturity. See Table 5 for descriptive statistics of the eight benchmark variables of interest. The majority of the organizations in the data set falls somewhere between a level 2 and level 3 stage of information security maturity. This shows that the majority of organizations are choosing to view information security strictly from a risk-analysis viewpoint with very little management and user understanding of information security threats and impacts. This result also shows that organizations are not placing a heavy focus of

information security on developing security-conscious information users and views the goal of information security as chiefly to demonstrate compliance with laws and regulations.

Table 5: Descriptive Statistics for Information Security Planning Integration			
	N	Mean	Std. Deviation
BMK1 *RoleInfoSec*	119	2.4538	1.26053
BMK2 *RoleInfoSecManager*	117	2.2308	1.14006
BMK3 *TopMgmtParticipation*	119	2.4286	1.02156
BMK4 *UserParticipation*	119	2.2521	0.91335
BMK5 *PerformanceCriteria*	119	2.6975	1.04601
BMK6 *InfoSecTriggers*	119	2.7731	0.72995
BMK7 *LevelInfoSecManager*	118	2.6610	1.03131
BMK8 *InfoSecManagerParticipation*	118	2.5000	1.11516
Average		2.4996	

Principle component factor analysis utilizing Varimax with Kaiser normalization rotation method was conducted on the three measurement instruments. Table 3 shows the results of factor analysis of the dependent variable. 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. While the items measuring detection is slightly below the 0.7 threshold, it is deemed close enough for continued use in this study. The total variance explained for the three remaining dependent variables is 71.681 percent. In addition to Cronbach's alpha calculations, the Average Variance Extracted (AVE) is evaluated. AVE is a more rigorous assessment of reliability with values greater the 0.5 shows acceptable levels of reliability. Table 3 shows the AVE values for each construct. The first factor, recovery, appears to measure perceptions related to the security function's ability to help the organization respond to any natural or man-made threats against the organization. The deterrence factor appears to measure perceptions related specifically to the training and monitoring of the end user and the end users' willingness to follow organization security policies. The detection factor appears to measure the security function's ability to identify security violations along with who committed the violation and how.

Table 6: Factor Analysis of Dependent Variable			
	Recovery	*Deterrence*	*Detection*
Corrective Measures	0.863	0.228	0.144
Understand DRP	0.922	0.235	0.138
Understand Continuity Plans	0.914	0.241	0.098
User Training	0.193	0.736	0.105
User Compliance	0.157	0.848	0.064
Understand Consequences	0.184	0.827	0.157
Users Disciplined	0.274	0.656	0.250
Discover Attacks Quickly	0.027	0.206	0.696
Identify Perpetrator	0.162	0.209	0.822
Identify How Breach Happened	0.133	0.000	0.765
Eigenvalue	4.398	1.464	1.307
Variance explained	26.448	26.270	18.963
Cronbach's alpha	0.933	0.824	0.695
AVE	0.882	0.654	0.619

Examination of Benchmark Variables

The information security planning integration construct is the central construct of the model under investigation. This construct is measured through the use of benchmarks variables and Nolan's theoretical lens of functions within organizations exhibiting stages of growth. This study theorizes that each stage of growth within the information

security function is identifiable by changes in role, planning orientation, user and management awareness, and status of information security. Table 7 shows the Pearson correlations between all benchmark variables. The correlation matrix shows benchmark variables 6 (triggers of implementation) and 7 are poorly correlation with the remaining six benchmark variables so these two variables are deleted from the final model. The Cronbach's alpha and AVE for the information security planning integration construct is 0.763 and 0.511 respectively which shows reasonable reliability.

Table 7: Pearson Correlation Matrix of Benchmark Variables

	BMK1	*BMK2*	*BMK3*	*BMK4*	*BMK5*	*BMK6*	*BMK7*	*BMK8*
BMK1	1.000							
BMK2	0.391**	1.000						
BMK3	0.446**	0.432**	1.000					
BMK4	0.384**	0.221**	0.570**	1.000				
BMK5	0.434**	0.465**	0.480**	0.338**	1.000			
BMK6	0.229*	0.164	0.177	0.251*	0.187	1.000		
BMK7	0.290	0.170	0.185	0.274*	0.265*	0.004	1.000	
BMK8	0.234*	0.103	0.279*	0.434**	0.304**	0.031	0.412**	1.000

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

V. DATA ANALYSIS

SmartPLS version 2.0 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 relationships between constructs.

The research model under investigation specifies that information security planning integration mediates the relationship between structure variables and the effectiveness variables. To tests for mediating effects, Baron and Kenny [1986] suggest a three-step approach. For mediating effects to be evaluated, there first must be a significant relationship between the independent variables and the three dependent variables. Then a relationship must be established between independent variables and mediating variable. Lastly, a relationship must be established between the mediating variable and the three dependent variables. So three PLS models are analyzed to test for significant effects. Table 8 shows the path coefficients and t-values for the three PLS models.

The first model examines the relationship between the structure variable and the effectiveness variables. The structure of information security management variable shows reasonable significance with two of the three effectiveness variables. The second model examines the relationship between the structure latent variables and the mediating variable: information security planning integration. Baron and Kenny's [1986] second condition for mediating effects is satisfied. The third model examines the relationship between the mediator variables and the three effectiveness variables. Baron and Kenny's [1986] third condition is met as the information security planning integration variable is significantly related to all three effectiveness variables.

Table 8: Results of Testing for Conditions of Mediating Effects

	Relationship	Beta	t-values
Model 1	*Management -> Recovery*	-0.193	1.730
	Management -> Deterrence	-0.322	2.547*
	Management -> Detection	-0.261	2.716**
Model 2	*Management -> Planning Integration*	-0.227	2.749**
Model 3	*Planning Integration -> Recovery*	0.359	3.332**
	Planning Integration -> Deterrence	0.484	6.447**
	Planning Integration -> Detection	0.276	3.026**

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

Figure 2 shows the results of testing the model for mediating effects with Tables 9 and 10 showing the path coefficients and resulting t-values. As expected, the path coefficients are significant. In order to test for a mediating effect between the management activities variable and the effectiveness variables, another PLS model is evaluated with the inclusion of the direct effects between the management activities variable and the effectiveness variables. Figure 3 shows the results of testing the model for direct effects between the management activities variable and the effectiveness variables. Tables 11 and 12 shows the path coefficients and t-values for the PLS model examining the direct effects between the management activities variable and the effectiveness variables. With the mediating variable in the model, the direct effect between management activities and the three effectiveness variables are all insignificant. This provides evidence of a partial mediating effect of information security planning integration on the relationship between the structure of information security management activities and the effective utilization of deterrence and detection strategies. Table 13 shows the results of hypothesis testing. T-values and levels of significance are not reported for the three hypothesis investigating mediation as these three hypotheses are assessed by examining the change in significance of the direct effects between the model without the mediating variable and the model with the mediating variable.

Table 9: Path Coefficients for Model with Mediating Effects

	MGMT	*Planning Integration*
MGMT	0	0
Planning Integration	-0.302	0
Recovery	0	0.355
Deterrence	0	0.481
Detection	0	0.272

Table 10: t-values for Path Coefficients for Model with Mediating Effects

	MGMT	*Planning Integration*
MGMT	0	0
Planning Integration	4.805	0
Recovery	0	3.388
Deterrence	0	7.061
Detection	0	2.568

Table 11: Path Coefficients for Model with Direct Effects Between Structure and Effectiveness

	MGMT	*Planning Integration*
MGMT	0	0
Planning Integration	-0.293	0
Recovery	0.084	0.383
Deterrence	-0.178	0.428
Detection	-0.187	0.210

Table 12: t-values for Model with Direct Effects Between Structure and Effectiveness

	MGMT	*Planning Integration*
MGMT	0	0
Planning Integration	3.612	0
Recovery	0.671	3.710
Deterrence	1.728	5.845
Detection	1.613	2.025

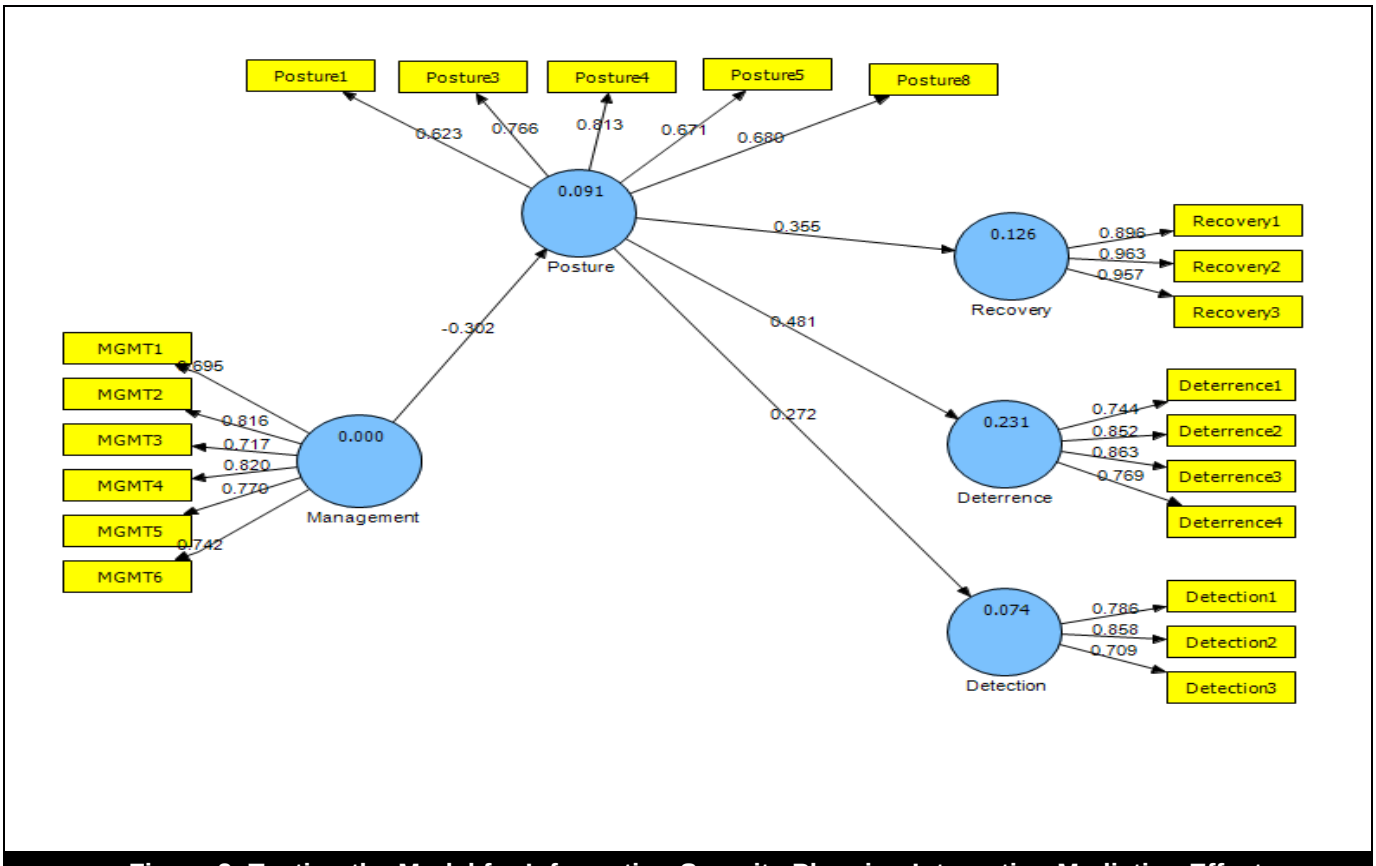

Figure 2: Testing the Model for Information Security Planning Integration Mediating Effects.

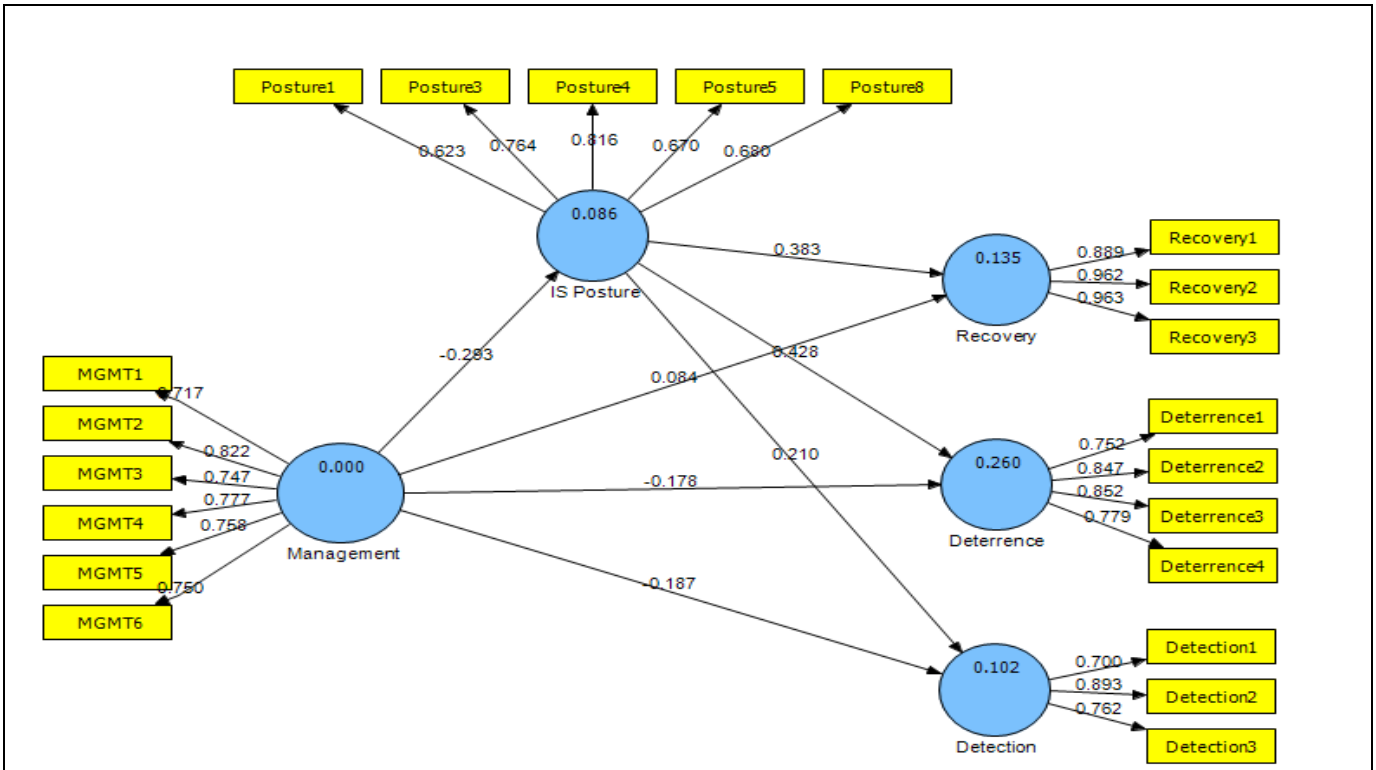

Figure 3:Testing for Direct Effects Between Structure and Effectiveness.

Table 13: Summary of Hypothesis Tests			
Hypothesis	Results	t-value	p-value
H_{a1a}: More advanced stages of information security planning integration are associated with higher levels of effectiveness of information security recovery measures.	Supported	3.332	0.0004
H_{a1b}: More advanced stages of information security planning integration are associated with higher levels of effectiveness of information security deterrence measures.	Supported	6.447	0
H_{a1c}: More advanced stages of information security planning integration are associated with higher levels of effectiveness of information security detection measures.	Supported	3.026	0.0012
H_{a2}: More advanced stages of information security planning integration are positively associated with more centralized information security management activities.	Not Supported	-2.749	0.997
H_{a3a}: Information security planning integration will mediate the impact of information security management activities on the effectiveness variables of information security recovery measures.	Not Supported	Not Applicable	
H_{a3b}: Information security planning integration will mediate the impact of information security management activities on the effectiveness variables of information security deterrence measures.	Supported	Not Applicable	
H_{a3c}: Information security planning integration will mediate the impact of information security management activities on the effectiveness variables of information security detection measures.	Supported	Not Applicable	

Hypothesis 1a-c proposes that organizations with more advances information security planning integration will more effectively utilize recovery, deterrence, and detection strategies. The results show that a significant positive relationship between maturity of the information security planning integration and effective utilization of three information security effectiveness strategies: recovery, deterrence, and detection. Organizations with more mature information security and business planning integration exhibit more sophisticated planning processes that include other management and user involvement which leads to more effective information security implementations. This finding is consistent with previous research that has shown user involvement in planning leads to better alignment between organization objectives and plans [Sambamurthy et al. 1994], higher user acceptance and buy-in [Lederer and Sethi 1991; Segars and Grover 1998; James 1996], greater extent of plan implementation [Gottschalk 1999] and better quality plans [Lederer and Mendelow 1987]. This finding is also consistent with previous research showing that a critical factor to success is how the organization views information security [Bjorck 2001].

Hypothesis 2 proposes that more centralized information security management activities are positively related to more mature information security and business planning integration. However, the results show a significant negative relationship between centralization of information security management and information security planning integration. This finding suggest that organizations with more sophisticated information security planning processes push the responsibilities of many information security activities down the corporate hierarchy. This pushing of responsibilities down the corporate ladder may be dependent on the size of the information security departments. More mature information security organizations may very well employ more specialized employees to handle specific information security activities. This finding suggests that how the organization chooses to structure activities of the information security function can impact the information security planning integration.

Hypothesis 3a–c proposes that the maturity of the organization's information security planning integration will mediate the relationship between the structure of information security management activities and the effective utilization of information security strategies. The results show partial mediation is present in the relationship between structure of information security management activities and deterrence and detection strategies. This result support previous research that organizational structure does not have a direct relationship with success variables [Fry 1982]. However, model testing shows no mediation is present in the relationship between the structure of information security management activities and the effective utilization of recovery strategies. This is an interesting result as it implies that how the organization chooses to structure the information security management activities does not impact the effectiveness of information security recovery strategies. Meanwhile, how the organization chooses to structure information security management activities is impacting the effectiveness of detection and deterrence strategies. Data analysis shows the information security planning integration construct explains a significant amount of the variance in the effective utilization of recovery, deterrence, and detection strategies.

VI. CONCLUSIONS

The results shows that the majority of organizations are choosing to view information security strictly from a cost-benefit or risk analysis viewpoint. Parker [2007], Gordon and Loeb [2006], and Dutta and McCrohan [2002] discuss the dangers of using risk analysis and cost-benefit analysis to examine information security investments and implementations. While cost-benefit analysis and risk analysis are great tools for regular occurring information security problems like virus attacks, these tools are poor for situational analysis that is more sporadic, like natural disasters (i.e., Hurricane Katrina, the great Chicago fire, etc.) or targeted attacks [Parker 2007]. It is good news that Gordon and Loeb [2006] find that organizations are gradually beginning to use economic analysis when examining information security investments.

The result also shows that organizations are not placing a heavy focus of information security on developing aware, responsible information users. Further evidence of the lack of emphasis on developing responsible information users within the organization is seen in the effectiveness measures. The only effectiveness measures that show a below neutral response dealt with user training providing further evidence that organizations are not placing enough emphasis on developing responsible information users. Verton [2002] finds that less than 50 percent of organizations have an IT security and training program for employees.

The findings also suggests that organizations' view the goal of information security is chiefly to demonstrate compliance with laws and regulations. This is not a surprising finding as liability is the number one concern of executives [Dutta and McCrohan 2002]. However, this is a very narrow, short-sighted viewpoint of information security, as laws and regulations are geared toward protecting external stakeholders of the organization like customers and investors. Information security strategies and investment are more effective when they are aligned with organizational mission and objectives [Backhouse and Dhillon 1996; James 1996; Parker 2007]. Laws and regulations are not focused on assisting management with the alignment of organizational objectives and information security strategies.

The results show that a significant positive relationship between maturity of the information security planning integration and effective utilization of three information security effectiveness strategies: recovery, deterrence, and detection. Organizations with more mature information security planning integration exhibit more sophisticated planning processes that include management and user involvement, which leads to more effective information security implementations. This finding is consistent with previous research that has shown user involvement in planning leads to better alignment between organization objectives and plans [Sambamurthy et al. 1994], higher user acceptance and buy-in [James 1996; Lederer and Sethi 1991; Segars and Grover 1998], greater extent of plan implementation [Gottschalk 1999], and better quality plans [Lederer and Mendelow 1987]. The findings suggest the best-performing organizations are those with more sophisticated information security planning processes where the role of information security is more focused on supporting the organization's mission and objectives and the performance structure encourages aligning information security investment with organizational objectives. This provides evidence for interpretive studies [Backhouse and Dhillon 1996; Baskerville 1991; Dhillon and Backhouse 2001; Parker 2007] that tout the critical nature of aligning information security initiatives with the organizations objectives.

There are several limitations to this paper. One limitation to this study is the broad, high-level view of information security is a simple representation of a very complex, deeply intertwined area of organizational behavior. This study also avoids examining the technical and functional details of the organization information security strategies, focusing instead on management practices. The technical infrastructure and prevention measures are clearly an important consideration in any study of information security within organizations and represent two issues ripe for future research. Another limitation is the cross-sectional design of the study which does not permit conclusions

about causation. Therefore, only claims of correlations among the variables of interest are possible. One final limitations is the low response rate may bias the final results.

VII. IMPLICATIONS FOR RESEARCH AND PRACTICE

This research supports the position of previous literature [Backhouse and Dhillon 1996; Baskerville 1991; Parker 2007] describing the importance of aligning information security objectives with overall business objectives. By integrating the information security and business planning activities, management can more effectively protect the organizational data and resources. This research also suggests that organizations with more decentralized information security management activities exhibit more mature information security planning integration. While prior research suggest that centralizations is the more effective approach to managing an organizations information security [Kotulic and Clark 2004], our findings support a vastly different conclusion. The complexity and uncertainty inherent within the information security domain is better managed through the decentralization of information security management activities. However, decentralizing a critical function can lead to problems when lower-level employees are incompetent to deal with the decision or lack guidance. To effectively deal with the potential problems in a decentralized environment, organizations must have strong planning integration. This research also offers some evidence that organizational functions can exhibit stages of maturity and that measurement is possible, giving some credence to often discussed maturity models discussed in the business world and among standards governing bodies (COBIT, CMM, and SOA MM). Future research examining the strategic aspiration of the information security function along internal environmental factors and organization's capabilities may help to better explain the variance in effectiveness of information security strategies among organizations.

VIII. SUMMARY

Our research hints that information security within organizations is improving as information security planning is becoming more integrated with overall business planning and the utilization of information security strategies are improving. Organizations recognize the value of integrating information security into the overall business planning processes to improve both the efficiency and effectiveness of protecting the information assets of the organization. Organizations employing more integrated planning processes allow the information security function to push more of the decision making down the hierarchy where decisions can be made closer to the problem.

REFERENCES

Editor's Note: The following reference list contains hyperlinks to World Wide Web pages. Readers who have the ability to access the Web directly from their word processor or are reading the paper on the Web, can gain direct access to these linked references. Readers are warned, however, that:

1. These links existed as of the date of publication but are not guaranteed to be working thereafter.
2. The contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.
3. The author(s) of the Web pages, not AIS, is (are) responsible for the accuracy of their content.
4. The author(s) of this article, not AIS, is (are) responsible for the accuracy of the URL and version information.

Adria, M., and S.D. Chowdhury (2004) "Centralization as a Design Consideration for the Management of Call Centers", *Information and Management* (41)4, pp. 497–507.

Aktinson, W. (2005) "Integrationg Risk Management and Information Security", *Risk Management* 5210, pp. 32–37.

Alloway, R.M., and J.A. Quillard (1983) "User Managers' Systems Needs", *Management Information Systems Quarterly* (7)2, pp. 27–43.

Backhouse, J., and G. Dhillon (1996) "Structures of Responsibility and Security of Information Systems", *European Journal of Information Systems* (5), pp. 2–9.

Baron, R.M., and D.A. Kenney (1986) "The Moderator-Mediater Variable Distinction in Social Psychological Research: Conceptual, Strategic, and Statistical Considerations", *Journal of Personality and Social Psychology* (51)6, pp. 1173–1182.

Baskerville, R. (1991) "Risk Analysis: An Interpretive Feasibility Tool in Justifying Information System Security", *European Journal of Information Systems* (1)2, pp. 121–130.

Baskerville, R. (1983) "Information Systems Security Design Methods: Implications for Information Systems Development", *ACM Computing Surveys* (25)4, pp. 375–414.

Benbasat, I, A.S. Dexter, and R.W. Mantha (1980) “Impact of Organizational Maturity on Information System Skill Needs”, *MIS Quarterl* (4)1, pp. 21–34.

Benbasat, I., et al. (1984) “A Critique of the Stage Hypothesis: Theory and empirical evidence”, *Communications of the ACM* (27)5, pp. 476–485.

Benjamin, R.I, C. Dickinson, and J.F. Rockart (1985) “Changing Role of the Corporate Information Systems Officer”, *MIS Quarterly,* (9)3, pp. 177–188.

Björck, F. (2001) “Implementing Information Security Management Systems—An Empirical Study of Critical Success factors” in *Advances in Information Security Management and Small Systems Security*, Eloff, J., L. Labuschagne, R. Solms, G. Dhillon (eds.) Klüwer Academic Publisher, Norwell, MA, pp. 197–211.

Bodin, L.D., L.A. Gordon, and M.P. Loeb (2005) “Evaluating Information Security Investments Using the Analytic Hierarchy Process”, *Communications of the ACM* (48)2, pp. 79–83.

Boynton, A.C., R.W. Zmud, and G.C. Jacobs (1994) “The Influence of IT Management Practice on IT use in Large Organizations”, *MIS Quarterly* (18)3, pp. 299–320.

Bradner, S. “The Winner So Far: Cardsystems Solutions”, *Network World* (2)25, p. 30.

Brown, I.T.J. (2004) “Testing and Extending Theory in Strategic Information Systems Planning Through Literature Analysis”, *Information Resources Management Journal* (17)4, pp. 20–48.

Byrne, B.M. (1998) *Structural Equation Modeling with LISREL, PRELIS, and SIMPLIS: Basic Concepts, Applications, and Programming*, Mahwah, NJ: Lawrence Erlbaum Associates.

Brynjolfsson, E. (1993) “The Productivity Paradox of Information Technology”, *Communications of the ACM* (36)12, pp. 67–77.

Byrd, T.A., V. Sambamurthy, and R.W. Zmud (1995) “An Examination of IT Planning in a Large, Diversified Public Organization”, *Decision Sciences* (26)1, pp. 49–73.

Cavusoglu, H., B. Mishra, and S. Raghunathan (2004) “A Model for Evaluating IT Security Investments”, *Communications of the ACM* (47)7, pp. 87–92.

Chang, S.E., L. Chin-Shien (2007) “Exploring Organizational Culture for Information Security Management”, *Industrial Management and Data Systems* (107)3, pp. 438–458.

Cheney, P.H., R.I. Mann, and D.L. Amoroso (1986) “Organizational Factors Affecting the Success of End-user Computing”, *Journal of Management Information Systems* (3)1, pp. 65–80.

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

Chin, W.W., B.L. Marcolin, and P.R. Newsted (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, pp. 189–217.

Da Veiga, A., and J.H.P. Eloff (2007) “An Information Security Governance Framework”, *Information Systems Management* (24), pp. 361–372.

Danziger, J.N., et al. (1993) “Enhancing the Quality of Computing Service”, *Public Administration Review* (53)2, pp. 161–170.

Dearden, J. (1972) “MIS Is a Mirage”, *Harvard Business Review* (50)1, pp. 90–99.

DeLone, W.H., and E.R. McLean (2003) “The DeLone and McLean Model of Information Systems Success: A Ten-Year Update”, *Journal of Management Information Systems* (19)4, pp. 9–30.

Dhillon, G., and J. Backhouse (2000) “Information System Security Management in the New Millennium”, *Communications of the ACM* (43)7, pp. 125–128.

Dhillon, G., and Backhouse, J. (2001) “Current Directions in IS Security Research: Towards Socio-organizational Perspectives”, *Information Systems Journal* (11)2, pp. 127–153.

Drury, D.H. (1983) “An Empirical Assessment of the Stages of DP Growth”, *MIS Quarterly* (7)2, pp. 59–70.

Dutta, A., and K. McCrohan (2002) “Management’s Role in Information Security in a Cyber Economy”, *California Management Review* (45)1, pp. 67–87.

Earl, M.J. (1993) “Experience in Strategic Information Systems Planning”, *MIS Quarterly* (7)1, pp. 1–24.

Ein-Dor, P., and E. Segev (1978) "Organizational Context and the Success of Management Information Systems", *Management Science* (24)10, pp. 1064–1077.

Ein-Dor, P., and E. Segev (1982) "Organizational Context and MIS Structure: Some Empirical Evidence", *MIS Quarterly* (6)3, pp. 55–68.

Fried, L. (1994) "Information Security and New Technology", *Information Systems Management* (11)3, pp. 57–63.

Fry, L.W. "Technology-Structure Research Three Critical Issues", *Academy of Management Journal* (25)3, pp. 532–552.

Galletta, D.F., and A.L. Lederer (1989) "Some Cautions on the Measurement of User Information Satisfaction", *Decision Sciences* (20)3, pp. 419–438.

George, J.F., and J.L King (1991) "Examining the Computing and Centralization Debate", *Communications of the ACM* (34)7, pp. 62–72.

Gopal, A., R.P. Bostrom, and W.W. Chin (1992–1993) "Applying Adaptive Structuration Theory to Investigate the Process of Group Support Systems Use", *Journal of Management Information Systems*,(9)3, pp. 45–69.

Gordon, L.A., and M.P. Loeb (2006) "Budgeting Process for Information Security Expenditures", *Communications of the ACM* (49)1, pp. 121–125.

Gottschalk, P. (1999) "Implementation Predictors of Strategic Information Systems Plans", *Information and Management* (36)2, pp. 77–91.

Govindarajan, V. (1986) "Decentralization, Strategy, and Effectiveness of Strategic Business Units in Multibusiness Organizations", *Academy of Management Review* (11)4, pp. 844–856.

Hair, J.F., et al. (1998) *Multivariate Data Analysis with Readings,* 5th edition, Englewood Cliffs, NJ: Prentice Hall.

Hartono, E., et al. (2003) "Key Predictors of the Implementation of Strategic Information System Plans", *Database for Advance in Information Systems* (34)3, pp. 41–53.

Henderson, J.C., and J.G. Sifonis (1988) "The Value of Strategic IS Planning: Understanding Consistency, Validity, and IS Markets", *MIS Quarterly* (12)2, pp. 187–200.

Hoffer, J.A., and D.W. Straub (1989) "The 9 to 5 Underground: Are You Policing Computer Crimes", *Sloan Management Review* (30)4, pp. 35–43.

Huff, S.L., M.C. Munro, and B.H. Martin (1988) "Growth Stages of End User Computing", *Communications of the ACM* (31)5, pp. 542–550.

Information Systems Audit and Control Association (ISACA) (2009) "An Introduction to the Business Model for Information Security", www.isaca.org/AMTemplate.cfm?Section=Deliverables&Template=/ContentManagement/ContentDisplay.cfm&ContentID=48017.

James, H.L. (1996) "Managing Information Systems Security: A Soft Approach", *Proceedings of the Information Systems Conference of New Zealand*, pp. 10–20.

Kankanhalli, A., et al. (2003) "An Integrative Study of Information Systems Security Effectiveness", *International Journal of Information Management* (23), pp. 139–154.

King, J.L. (1983) "Centralized Versus Decentralized Computing: Organizational Considerations and Management Options", *Computing Surveys* (15)4, pp. 319–349.

King, W.R., and K.L. Kraemer (1984) "Evolution and Organizational Information Systems: An Assessment of Nolan's Stage Model", *Communications of the ACM* (27)5, pp. 466–475.

King, W.R., and T.S.H. Teo (1997) "Integration Between Business Planning and Information Systems Planning: Validating a Stage Hypothesis", *Decision Sciences* (28)2, pp. 279–308.

Kotulic, A., and J.G. Clark (2004) "Why There Aren't More Information Security Research Studies", *Information and Management* (41)5, pp. 597–607.

Kwok, L., and D. Longley (1999) "Information Security Management and Modeling", *Information Management & Computer Security* (7)1, pp. 30–46.

Lederer, A.L., and A.L. Mendelow (1987) "Information Resource Planning: Overcoming Difficulties in Identifying Top Management's Objectives", *MIS Quarterly* (11)3, pp. 389–399.

Lederer, A.L., and H. Salmela (1996) "Toward a Theory of Strategic Information Systems Planning", *Journal of Strategic Information Systems* (5), pp. 237–253.

Lederer, A.L., and V. Sethi (1988) “The Implementation of Strategic Information Systems Planning Methodologies”, *MIS Quarterly* (12)3, pp. 445–461.

Lederer, A.L., and V. Sethi (1991) “Critical Dimensions of Strategic Information Systems Planning”, *Decision Sciences* (22)1, pp. 104–119.

Lederer, A.L., and V. Sethi (1992) “Root Causes of Strategic Information System Planning Implementation Problems”, *Journal of Management Information Systems* (9)1, pp. 25–46.

Lederer, A.L., and V. Sethi, “Key prescriptions for strategic information system planning”, *Journal of Management Information Systems,* 1996, 13:1, pp. 35–62.

Lee, B., A. Barua, and A.B. Whinston (1997) “Discovery and Representation of Casual Relationships in MIS Research: A Methodological Framework”, *MIS Quarterly* (21)1, pp. 109–136.

Loch, K.D., H.H. Carr, and M.E. Warkentin (1992) “Threats to Information Systems: Today’s Reality, Yesterday’s Understanding”, *MIS Quarterly* (16)2, pp. 173–185.

Lucas Jr., H.C., and J.A. Sutton (1977) “The Stage Hypothesis and the S-curve: Some Contradictory Evidence”, *Communications of the ACM* (20)4, pp. 254–259.

Magal, S.R., H.H. Carr, and H.J. Watson (1988) “Critical Success Factors for Information Center Managers”, *MIS Quarterly* (12)3, pp. 413–425.

Mahmood, M.A., and J.D. Becker (1985–1986) “Effects of Organizational Maturity on End Users’ Satisfaction with Information Systems”, *Journal of Management Information Systems* (2)3, pp. 37–64.

McFarlan, F.W., J.L. McKenney, and P. Pyburn (1983) “The Information Archipelago—Plotting a Course”, *Harvard Business Review* (61)1, pp. 145–156.

Miller, D., and P.H. Friesen (1984) “A longitudinal study of the corporate life cycle”, *Management Science* (30)10, pp. 1161–1183.

Moch, M.K., and E.V. Morse (1977) “Size, Centralization, and Organizational Adoption of Innovations”, *American Sociological Review* (42)5, pp. 716–725.

Nault, B.R. (1998) “Information Technology and Organization Design: Locating Decisions and Information”, *Management Science* (44)10, pp. 1321–1335.

Nolan, R.L. (1973) “Managing the Computer Resource: A Stage Hypothesis”, *Communications of the ACM* (16)7, pp. 399–405.

Nolan, R.L. (1979) “Managing the Crisis in Data Processing”, *Harvard Business Review* (57)2, pp. 115–126.

Olson, M.H., and N.L. Chervany (1980) “The Relationship Between Organizational Characteristics and the Structure of the Information Services Function”, *MIS Quarterly* (4)2, pp. 57–68.

Pattinson, M.R., G. Anderson (2007) “How Well Are Information Risks Being Communicated to Your Computer End-users?” *Information Management and Computer Security* (15)5, pp. 362–371.

Parker, D.B. (2007) “Risks of Risk-based Security”, *Communications of the ACM* ,(50)3, p. 120.

Peffers, K., C.E. Gengler, and T. Tuunanen (2003) “Extending Critical Success Factors Methodology to Facilitate Broadly Participative Information Systems Planning”, *Journal of Management Information Systems* 201, pp. 51–85.

Pimchangthong, D., M. Plaisnet, and P. Bernard (2003) “Key Issues in Information Systems Management: A Comparative Study of Academics and Practitioners in Thailand”, *Journal of Global Information Technology Management* (6)4, pp. 27–44.

Premkumar, G., and W.R. King (1994) “Organizational Characteristics and Information System Planning: An Empirical Study”, *Information Systems Research* (5)2, pp. 75–109.

Pyburn, P.J. (1983) “Linking the MIS Plan with Corporate Strategy: An Exploratory Study”, *MIS Quarterly* (7)2, pp. 1–14.

Reich, B.H., and I. Benbasat (1996) “Measuring the Linkage Between Business and Information Technology Objectives”, *MIS Quarterly* (20)1, pp. 55–81.

Sabherwal, R. (1999) “The Relationship Between Information System Planning Sophistication and Information System Success: An Empirical Assessment”, *Decision Sciences* ,(30)1, pp. 137–167.

Sambamurthy, V., R.W. Zmud, and T.A. Byrd (1994), "The Comprehensiveness of IT Planning Processes: A Contingency Approach", *Journal of Information Technology Management* (5)1, pp. 1–10.

Schultz, E.E., et al. (2001) "Usability and Security—An Appraisal of Usability Issues in Information Security Methods", *Computers & Security* (20)7, pp. 620–634.

Seddon, P.B., et al., (1999) "Dimensions of Information Systems Success", *Communications of the Association of Information Systems* (2)20, pp. 2–60.

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

Shimeall, T.J., and J.J. McDermott (1999) "Software Security in an Internet World: An Executive Summary", *IEEE Software* ,(16)4, pp. 58–62.

Siponen, M., "Toward Maturity of Information Security Maturity Criteria: Six Lessoned Learned from Software Maturity Criteria", *Information Management & Computer Security* (10)5, pp. 210–224.

Stanton, J.M., et al. (2003) "Examining the Linkage Between Organizational Commitment and Information Security", *International Conference Systems, Man and Cybernetics* (3) pp. 2501–2506.

Straub, D.W., and R.J. Welke (1998) "Coping with Systems Risk: Security Planning Models for Management Decision Making", *MIS Quarterly* 224, pp. 441–469.

Tavakolian, H. (1989) "Linking the Information Technology Structure with Organizational Competitive Strategy: A Survey", *MIS Quarterly* (13)3, pp. 309–317.

Teo, T.S.H., and J.S.K. Ang (2001) "An Examination of Major IS Planning Problems", *International Journal of Information Management* (21), pp. 457–470.

Thong, J.Y.L., C.S. Yap, and K.S. Raman (1996) "Top Management Support, External Expertise and Information Systems Implementation in Small Businesses", *Information Systems Research* (7)2, pp. 248–267.

Venkatesh, V., et al. (2003) "User Acceptance of Information Technology: Towards a Unified View", *MIS Quarterly* (27)3, pp. 425–478.

Verton, D. (2002) "Disaster Recovery Planning Still Lags", *ComputerWorld* (36)14, p. 10.

Wade, J., 2004 "The weak link in IT security", *Risk Management,* , 51:7, pp. 32–37.

Wylder, J.O.D. 1992 "The Life Cycle of Security Managers", *Information Systems Management* ,(9)1, pp. 62–68.

Von Solms, B. (2000) "Information Security—The Third Wave", *Computers & Security* (19)7, pp. 615–620.

Zmud, R.W. (1982) "Diffusion of Modern Software Practices: Influence of Centralization and Formalization", *Management Science* (28)12, pp. 1421–1431.

ABOUT THE AUTHORS

Randall F. Young is an assistant professor in the department of accounting and business law at the University of Texas–Pan American. His research interest includes IT infrastructure and information security management. He earned a Ph.D. in Computer Information Systems from the University of North Texas, a master's of accountancy from Abilene Christian University, and a BBA in Finance from the University of Texas at Arlington. He has published in *Information Resource Management Journal*, *Information Systems Management* and *Journal of Organizational and End User Computing*.

John C. Windsor is a professor of Information Systems and former Director of the Information Systems Research Center at the University of North Texas. He received his Ph.D. in Decision Sciences from Georgia State University. He has published over six books and sixty articles in such journals as *Data Base*, *IIE Transactions*, *Information & Management* and *Computers & Security*. His research interests include software and data engineering, systems security, collaborative computing, and the organizational impact of information technology.

Communications of the Association for Information Systems

ISSN: 1529-3181

Communications of the Association for Information Systems