Information Management & Computer Security

Emerald Article: Impacts of organizational capabilities in information security

Jacqueline H. Hall, Shahram Sarkani, Thomas A. Mazzuchi

The current issue and full text archive of this journal is available at
www.emeraldinsight.com/0968-5227.htm

Impacts of organizational capabilities in information security

Jacqueline H. Hall, Shahram Sarkani and Thomas A. Mazzuchi
Department of Engineering Management and Systems Engineering, The George Washington University, Washington, DC, USA

Received 8 November 2010
Revised 7 January 2011
Accepted 14 February 2011

Abstract

Purpose – This research aims to examine the relationship between information security strategy and organization performance, with organizational capabilities as important factors influencing successful implementation of information security strategy and organization performance.

Design/methodology/approach – Based on existing literature in strategic management and information security, a theoretical model was proposed and validated. A self-administered survey instrument was developed to collect empirical data. Structural equation modeling was used to test hypotheses and to fit the theoretical model.

Findings – Evidence suggests that organizational capabilities, encompassing the ability to develop high-quality situational awareness of the current and future threat environment, the ability to possess appropriate means, and the ability to orchestrate the means to respond to information security threats, are positively associated with effective implementation of information security strategy, which in turn positively affects organization performance. However, there is no significant relationship between decision making and information security strategy implementation success.

Research limitations/implications – The study provides a starting point for further research on the role of decision-making in information security.

Practical implications – Findings are expected to yield practical value for business leaders in understanding the viable predisposition of organizational capabilities in the context of information security, thus enabling firms to focus on acquiring the ones indispensable for improving organization performance.

Originality/value – This study provides the body of knowledge with an empirical analysis of organization's information security capabilities as an aggregation of sense making, decision-making, asset availability, and operations management constructs.

Keywords Information security, Organizational performance, Organizational capabilities, Strategy implementation success, Structural equation modeling, Strategic management

Paper type Research paper

1. Introduction

Despite increasing investment in information security and its strategic role in today's business success, effective implementation of information security strategy still remains one of the top challenges facing global organizations (Ernst & Young, 2007, 2008; Fratto, 2009; TechAmerica, 2009; PricewaterhouseCoopers, 2008). Business has been urged to make information security, a strategic issue for organizations to compete

This work was based on a conference paper titled "Moderating roles of organizational capabilities in information security", which was presented by the authors at the 5th International Conference on i-Warfare and Security (ICIW 2010), 8-9 April 2010, Dayton, Ohio.

Information Management & Computer Security
Vol. 19 No. 3, 2011
pp. 155-176

0968-5227
DOI 10.1108/09685221111153546

and survive in this era of global economy and ever changing enterprise risk (Wood, 1993; Ezingeard *et al.*, 2005; Amaio, 2009). Success in such demanding business environments depends in large part on implementing an effective information security strategy to protect information and information assets. Recent information security literature recommends organizations employ an overall information security strategy that integrates "people, processes, technology, and operations capabilities" to ensure effective defenses across the organization (Allen, 2005; FFIEC, 2006; NIST, 2008). Additionally, today's global connectedness and rapidly advancing information technologies have made technology-driven security solutions inadequate to meet information security challenges (Caralli, 2004; Alberts *et al.*, 2001; Alberts and Hayes, 2003). In order to face the challenges and to take advantage of new opportunities brought forth by information technology advances, Caralli (2004) suggests organizations shift the focus from a technology-based information security strategy to an organizational-based approach that considers a core set of organizational capabilities. Therefore, the identification and understanding of organizational capabilities is essential to logically recognize the relationship between information security strategy implementation success and organization performance.

For the purpose of this study, organizational capabilities are defined as intangible assets consisting of competencies along with dynamics of integrating and deploying those competencies with inimitable resources across organizational boundaries to operate business. Competencies refer to differentiated knowledge, skill, ability, distinctive organizational processes, and other characteristics needed to perform a specific task. The resources in this study include human, physical, financial, and technological resources. It is necessary to note that during the course of the literature review, no theoretical model was found that combined these variables or one that resembled the theoretical model illustrated in this research.

The overall objective of this research is to address two information security related issues. First, in today's complex, competitive, and dynamic marketplace, organizations may not be equally predisposed for effective implementation of information security strategy. Key to information security strategy implementation success within organizations is the identification and assessment of preconditions necessary to attain strategic goals. These preconditions refer to an organization's capabilities, the means by which information security strategy gets implemented. Organizations need to have a clear understanding of the minimum essential capabilities required for effective information security strategy and build the ones indispensable for creating business value.

Second, information security is an interdisciplinary field encompassing organizational, managerial, and technical aspects (von Solms, 2006; Werlinger *et al.*, 2009). Most prior research efforts on information security have been traditionally dedicated to the technical or managerial side (Chang and Ho, 2006; Kankanhalli *et al.*, 2003; Knapp *et al.*, 2006). Additionally, while the emerging academic and industry perspective is to emphasize the alignment of information security strategy to business strategy and objectives that supports the paradigm shift from a technical role toward a value-creating role (Allen, 2005; Caralli, 2004; Huang and Hu, 2007; Rathnam *et al.*, 2004; Ezingeard *et al.*, 2005), little emphasis has been devoted to understanding the role of organizational capabilities as potential sources of sustainable competitive advantage. Specifically, no research to date has yet looked at organizational capabilities as the fundamental determinants of the potential association between information security strategy implementation success and

organization performance. As a result, the organizational aspect is still largely unexplored. Among the limited number of studies concerning organizational capability, few have empirically analyzed organizational capability as a multidimensional construct (Kusunoki *et al.*, 1998). In particular, with the exception of research studies discussing these constructs as best practices in information security management literature, there has been almost no evidence of information security research devoted to empirical analysis of organizational capability as an aggregation of sense making, decision making, asset availability, and operations management constructs.

2. Theoretical foundation

In the last decade, information and information security have moved beyond the boundaries of academia to play key roles to improve overall business objectives and create competitive advantage (Saugatuck Technology, 2008; Schultz, 2006; Tallon *et al.*, 2000; Wood, 1993). More and more businesses around the world now regard information as a vital business asset critical to the success of organizations in today's globally connected and complex business environment (Straub, 1990; FFIEC, 2006; McFadzean *et al.*, 2007; Kaplan and Norton, 2007). As such, information security is more challenging now than ever before to defend a business against increasingly sophisticated information security threats (Anderson and Choobineh, 2008; Park and Ruighaver, 2008; Symantec, 2009). Indeed, according to Allen (2005), "national and international regulations are calling for organizations to demonstrate due care with respect to security". This is crucial to providing an agile and trusted environment for organizations to compete and survive in the current marketplace. An organization can benefit from its ability to protect information and the environment in which it exists. Among these benefits are, maintaining compliance with the law, preserving brand strength, and company reputation, increasing customer trust, sustaining business resiliency, and thereby achieving organizational objectives and improving business performance (Caralli, 2004; van Opstal and Council on Competitiveness, 2007; Nyanchama, 2005; NIST, 2007; Ezingeard *et al.*, 2005; Kim, 2004).

The challenges of a competitive marketplace with constantly changing business requirements and the upward trend of cyber threats are realizing the need for a more strategic view of information security (Kankanhalli *et al.*, 2003; Park and Ruighaver, 2008; Straub, 1990). NIST (2008) suggests that, "to mitigate risk from the global supply chain, a comprehensive information security strategy should be considered that employs a strategic, organization-wide, defense-in-breadth approach." Lack of a proactive information security strategy to make information available, accessible, assured, and appropriately protected can disrupt operations and pose serious risks to the organization's performance and competitiveness as well as to those of customers (Fratto, 2009; Wood, 1993; FFIEC, 2006; Allen, 2005). In addition, despite technical advances that provide existing tools to protect information assets, technology alone is not sufficient as information security threats and vulnerabilities have also increased (Alberts, 2003; Deloitte, 2008; ISACA, 2009). Success in meeting these challenges necessitates business focus on the preconditions that are critical to the effective implementation of information security strategy to protect and defend information assets against adversarial threats on compromising confidentiality, integrity, and availability. As such, Alberts and Hayes (2003) propose a framework for identifying "the shortcomings of existing force structure, concepts of operations, personnel, education, training, material, and systems" by looking at the minimum essential preconditions required for successful operations.

This framework consists of the ability to make sense of the situation, the ability to work in a coalition environment, the ability to possess appropriate means, and the ability to orchestrate the means to respond in a timely manner. Although the focus of Albert and Hayes's framework is on military and government, this framework can also apply to other organizations as they will likely encounter similar shortcomings facing challenges of today's fast advancing information technologies and increasingly sophisticated threat environments.

In general, these preconditions are designated as capabilities, within the classical strategic management and organizational theory literature (Gold *et al.*, 2001; Kelly and Amburgey, 1991; Wernerfelt, 1984; Teece *et al.*, 1997; Prahalad and Hamel, 1990; Barney, 1991; Barney and Zajac, 1994). The concept of organizational capabilities has been the focus of research in the field of strategic management and organizational theory, even though it has various definitions (Ansoff, 1965; Porter, 1985; Ulrich and Lake, 1991; Grant, 1991; Stalk *et al.*, 1992; Kusunoki *et al.*, 1998; Rangone, 1999; Eisenhardt and Martin, 2000; Ulrich and Smallwood, 2004; Smallwood and Panowyk, 2005; Wethyavivorn *et al.*, 2009). Regardless of the various classifications, most research shares the same viewpoint that organizational capabilities have the potential to become a source of sustainable competitive advantage, and that they are difficult to imitate and substitute (Barney, 1991; Collis, 1994; Teece *et al.*, 1997; Kusunoki *et al.*, 1998).

Over the years, numerous studies in strategic management have indicated that strategy is critical for achieving business objectives and competitive advantage (Porter, 1985; Prahalad and Hamel, 1990; Cockburn *et al.*, 2000; Eisenhardt and Martin, 2000; Slater and Olson, 2001). However, as Smallwood and Panowyk (2005) suggest, it is capabilities that give stakeholders confidence that an organization can develop and execute its strategy. Smallwood and Panowyk emphasize further that a business gains advantage only when it possesses appropriate organizational capabilities that "drive every aspect of performance, including customer satisfaction, competitive positioning, and bottom-line results". The resource-based view of strategy also reaffirms the strategic importance of organizational capabilities in enabling firms to plan, formulate, and implement their strategies (Barney and Zajac, 1994). Indeed, according to Ulrich and Smallwood (2004), organizational capabilities are what people respect most and expect from successful companies, not their organizational structure or their specific approaches to management. Additionally, Ulrich and Smallwood theorize that capabilities cannot be built independent of leadership. Besides, leadership, Ulrich and Smallwood (2004) also suggest some other capabilities organizations must possess to be able to carry out its missions and objectives. These capabilities include talent, speed, shared mind-set and coherent identity, accountability, collaboration, innovation, and efficiency:

RQ1. What is the relationship, if any, between information security strategy and organization performance?

RQ2. What are the relationships, if any, between organizational capabilities and information security strategy?

Together, the perspectives of the prior work by Alberts and Hayes (2003) and Ulrich and Smallwood (2004) coupled with information security literature given by Allen (2005), Caralli (2004), FFIEC (2006), and NIST (2008) provide a useful theoretical foundation for defining the constructs of the theoretical model. These include

information security strategy implementation success, organizational performance, sense-making, decision-making, asset availability, and operations management.

Information security strategy implementation. The degree to which information security programs protect and defend information and information systems against adversary threats on compromising the confidentiality, integrity, and availability, allow for better control of information assets, respond promptly to and recover quickly from information security attacks, while complying with legal, statutory, contractual, and internally developed requirements (NIST, 2008; FFIEC, 2006).

Organization performance. The degree to which organizations produce and accomplish business objectives and values for the various stakeholders. This includes preventing costly legal action related to the protection of information assets from government agencies, stockholders or others, improving customers service, preserving public's perception of brand strength or company reputation, and market valuation, while maintaining business resiliency in the face of an increasingly sophisticating risk environment (Alberts and Hayes, 2003; Ulrich and Smallwood, 2004).

Sense-making. The ability to develop high-quality awareness and understanding of current and future threats and vulnerabilities, social, political, and economical challenges, coupled with the organization's missions and constraints (Alberts and Hayes, 2003; Ulrich and Smallwood, 2004).

Decision-making. The ability to make decisions with respect to courses of action and planning, to collaborate, empower, and communicate information security strategy, as well as to commit to information security initiatives in support of the missions and business functions of organizations (NIST, 2007; Ulrich and Smallwood, 2004; Alberts and Hayes, 2003).

Asset availability. The ability to obtain and organize the competencies and processes needed to accomplish information security strategy goals and ensure employees have the necessary skills and resources to achieve it (NIST, 2007; Alberts and Hayes, 2003; Caralli, 2004; Allen, 2005).

Operations management. The ability to manage and deploy the combined competencies and resources across the organization in support of information security operations. This also involves the ability to measure and learn over time about risks and the operational environment for continuous improvement to information security programs (NIST, 2007; Ulrich and Smallwood, 2004; Alberts and Hayes, 2003).

3. Research model and hypotheses

In efforts to contribute to the existing body of literature about the organizational aspect of information security, this study seeks to address the research questions concerning the relationships between essential organizational capabilities, successful implementation of information security strategy, and organization performance. As such, the following hypotheses were offered:

H1. Successful implementation of an overall information security strategy is positively associated with organization performance.

H2. Sense-making is positively associated with information security strategy implementation success.

H3. Decision-making is positively associated with information security strategy implementation success.

H4. Asset availability is positively associated with information security strategy implementation success.

H5. Operations management is positively associated with information security strategy implementation success.

The study is accomplished by proposing and validating a theoretical model that demonstrates the linkage between effective implementation of information security strategy and organization performance, with organizational capabilities as important factors influencing this relationship. As shown in Figure 1, information security strategy implementation success is affected by organizational capabilities in terms of sense-making, decision-making, asset availability, and operations management, and in turn influences organization performance. These hypothesized relationships correspond to paths *H1*, *H2*, *H3*, *H4*, and *H5*, respectively, which are represented graphically by one-headed arrows as shown Figure 1.

4. Research methodology

4.1 Survey instrument

After an extensive review of literature, an original survey instrument was created to collect quantitative data for this study. The initial version of the survey was submitted to two survey methodologists for peer and technical reviews. Based on feedback and consideration of comments in the reviews, the questionnaire was revised and was subsequently used in pretesting.

Prior to field deployment of the survey instrument, a pretest was conducted with a small group of information technology professionals. This was necessary to ensure the

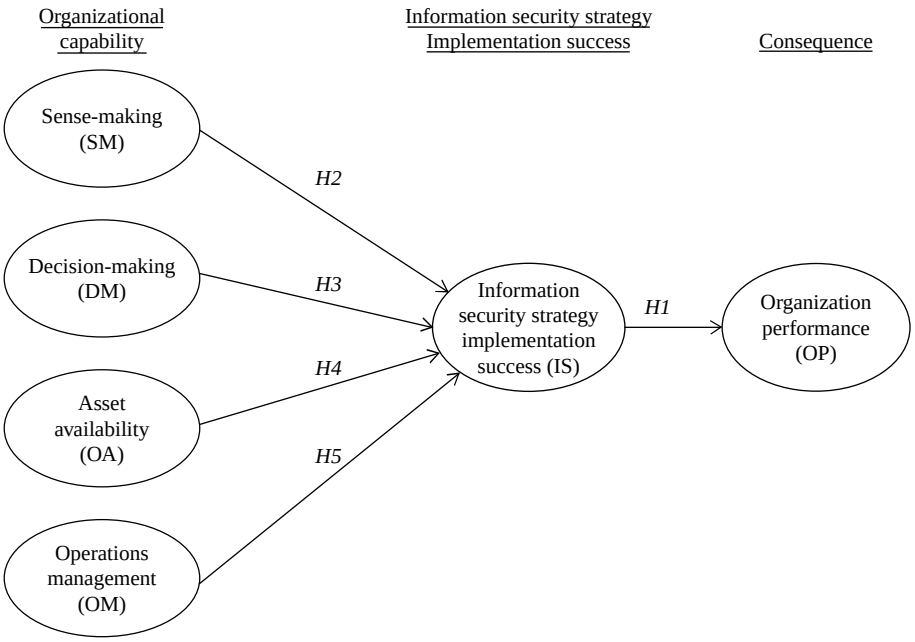

Figure 1.
Hypothesized model

questionnaire and instructions could be well understood and the response categories were comprehensive, and to assess whether any items or item wording may unnecessarily increase the respondent's burden in completing the survey (Bourque and Fielder, 2003). Results of the pretest were evaluated and applied in refining the questionnaire and the study design.

The final survey instrument consisted of 50 items and was divided into three sections. The first section comprised of 43 items and was further divided into six scales intended to measure the conceptual constructs. This section aimed at identifying the relationships between variables by asking respondents to rate the affirmative statements using a five-point Likert measurement scale. The questionnaire items and associated constructs are presented in Table I. The second section encompassed seven questions intended to obtain general demographic information. This includes respondent's security certifications, level of involvement in information security, job function, and years of experience, along with organization's industry, revenues, and number of employees. The third section contained a qualitative box provided for optional comments. Respondents may use the provided space to share additional thoughts not necessarily related directly to the research inquiry.

4.2 Sample and data collection

To collect empirical data essential for the validation of the underlying hypotheses, the final paper questionnaire was mailed to 1,600 respondents residing within the USA and the District of Columbia. The targeted sample population consists of Certified Information System Security Professionals (CISSPs), who may have a strong background and years of experience in information technology and information security. The name and contact information of respondents were selected at random and compiled from the publicly available International Information Systems Security Certification Consortium member directory.

4.3 Data analysis

Following data collection, analyses were conducted using a two-phase process consisting of confirmatory measurement model and confirmatory structural model suggested by Anderson and Gerbing (1988). The first phase involves confirmatory factor analysis that evaluates the measurement model on multiple criteria such as internal reliability, convergent, and discriminant validity. The second phase involves latent variables structural equation modeling (SEM) to test the hypothesized relationships and to fit the structural model. Predictive Analytics Software and Analysis of Moment Structures were utilized as the tools for analyzing data and conducting SEM discussed herein.

5. Analyses and results

5.1 Sample characteristics

It is noted that electronic surveys were mailed to 130 respondents in a pilot test. However, only 11 e-surveys were completed and returned. Owing to such low response rate, e-surveys were discarded. Of the 1,600 paper surveys, the researchers received 433 samples of responses from interested participants, of which five were dropped due to incomplete data. This resulted in 428 usable samples demonstrating a reasonable sample size required for the data analysis method employed in this study. In terms of information security qualifications, about 99.1 percent of the usable samples were from

Item	Description	Construct
SM1	Assesses the environmental impacts (i.e. social, political and economical) on information security	Sense making (SM)
SM2	Uses a systematic process to identify potential adversary actions or reactions	
SM3	Analyzes available information to determine risks to the enterprise	
SM4	Keeps current on the evolving capabilities of attackers and potential attackers	
SM5	Keeps decision makers informed of vital information security developments	
SM6	Provides appropriate security education and awareness on information assets protection	
DM1	Aligns information security objectives with the overall business goals	Decision making (DM)
DM2	Illustrates clear intention to support information security initiatives	
DM3	Links organizational governance structure to information security governance to provide consistency in planning, implementing, and delivering security in the organization	
DM4	Commits appropriate resources to achieve information security objectives	
DM5	Promotes workforce collaboration to protect business assets from information security attacks	
DM6	Takes measures to build a more competent enterprise that can defend business against increasingly sophisticated information security threats	
DM7	Communicates clear vision to mitigate information security risks	
OA1	Deploys an integrated combination of competencies and resources to protect information assets (competencies refer to knowledge, skill, and ability needed to perform a specific task)	Asset availability (OA)
OA2	Recruits people with appropriate information security competencies	
OA3	Retains a cadre of trained information security professionals	
OA4	Uses formal mechanisms such as training, policies, procedures, processes and technologies to ensure a secure, reliable, responsive, and trusted information technology environment	
OA5	Uses formal mechanisms such as policies, procedures, processes and technologies to enforce information security compliance	
OA6	Implements necessary procedures to ensure effective configuration management of all changes to information related systems	
OA7	Ensures continuity of mission-critical operations through contingency planning	
OA8	Reviews information security policy regularly to ensure its adequacy	
OA9	Provides a balance between security controls and access to information	
OM1	Assigns all security controls needed to protect the mission/business processes to responsible parties with accountability for development, implementation, and assessment	Operations management (OM)
OM2	Uses project management best practices to manage information security programs	
OM3	Uses metrics to identify the achieved security performance in its operational environment	
OM4	Uses metrics to increase accountability through the collection, analysis, and reporting of relevant performance-related data	

Table I.
Questionnaire items and intended constructs

(*continued*)

Item	Description	Construct
OM5	Uses metrics to facilitate DM	
OM6	Documents incidents to provide lessons learned that help modify information security strategy	
IS1	Maintains appropriate protection of information assets	Information security strategy implementation success (IS)
IS2	Achieves information security compliance with legislation, regulatory or industry requirements	
IS3	Upholds information security policies and standards	
IS4	Responds promptly to information security attacks	
IS5	Recovers quickly following system failure or interruption	
IS6	Keeps information security risks to a minimum	
IS7	Sustains continuity of mission-critical operations	
IS8	Prevents damages to information assets	
IS9	Allows for better control of information assets	
OP1	Increases customer trust	Organization performance (OP)
OP2	Prevents costly legal action from government agencies, stockholders, or others	
OP3	Preserves public's perception of brand strength or company reputation	
OP4	Improves customer service	
OP5	Preserves market valuation	
OP6	Maintains business resiliency in the face of a constantly changing risk environment	

Table I.

respondents possessing one more security certifications, of which 96.7 percent specified as CISSPs. Regarding job duties, 85.5 percent of respondents were directly involved in information security, 13.3 percent indirectly involved, and 1.2 percent not involved at all. Furthermore, 84.8 percent of respondents identified as having more than eight years of experience in information technology/information security. With respect to the organization's size, 54.7 percent of respondents were from companies with 5,000 or more employees. Additionally, the revenues profile of the usable samples also biased toward larger organizations with 56.3 percent having annual revenues of over $100 million. Moreover, the survey participants were well representative of firms across different industry types/sectors. These include government/non-profit (116), information communications and technology (94), insurance, financial, banking (76), healthcare, medical, pharmaceuticals (28), education/training (20), retail/wholesale (18), manufacturing/industrial (15), engineering (14), utilities (12), and other (35). Table II presents the demographic data of the samples represented in this study.

5.2 Confirmatory measurement model

Before the scales were subject to confirmatory factor analysis, factor loadings for each observed variable were examined to identify the correlation of that variable to the underlying construct in order to define the factor structure (Hair *et al.*, 2006). In confirmatory factor analysis, the constructs, known as latent variables or factors, are unobserved variables and are inferred by the respective questionnaire items, also termed observed variables. Principle axis factoring with varimax rotation method was conducted

Characteristics	Count	%
Security certification		
CISSP	414	96.7
Other	10	2.3
None	4	0.9
Level of involvement in information security		
Directly involve	366	85.5
Indirectly involve	57	13.3
Do not involve at all	5	1.2
Years of experience		
Less 5-8 years	7	1.6
Between 5 and 8 years	58	13.6
Between 8 and 15 years	159	37.1
More than 15 years	208	47.7
Job function		
Architecture and engineering	34	7.9
Budget, finance or accounting	1	0.2
Information technology/information security	317	74.1
Management/strategic planning	27	6.3
Operations/production	7	1.6
Sales and marketing	14	3.3
Organization industry		
Aerospace/engineering	14	3.3
Agriculture/chemicals	2	5
Consumer products/retail/wholesale/distributor	18	4.2
Education/training	20	4.7
Energy/utilities	12	2.8
Government/non-profit	116	27.1
Healthcare/medical/pharmaceuticals	28	6.5
Information/communications/technology	94	22.0
Insurance/financial/banking services	76	17.8
Manufacturing/industrial	15	3.5
Oil/gas/consumable fuels	2	0.5
Other	31	7.2
Number of employees		
15,000 or more	169	39.5
10,000-14,999	32	7.5
5,000-9,999	33	7.7
1,000-4,999	87	20.3
500-999	26	6.1
100-499	46	10.7
Less than 100	35	8.2
Organization revenues		
$1 billion or more	170	39.7
$500-$999.99 million	35	8.2
$100-$499.99 million	36	8.4
$50-$99.99 million	27	6.3
$10-$49.99 million	26	6.1
$5-$9.99 million	14	3.3
$1-$4.99 million	18	4.2
Less than $1 million	10	2.3
Do not know	92	21.5

Table II.
Demographic data

to compute the factor loading matrix. Items with significant cross loadings or loadings below the general cut-off value of 0.4 should be removed (Hair *et al.*, 2006).

As shown in Table III, all items demonstrated higher loadings with their corresponding factors, with the exception of items SM1, OA6, OA7, OA8, OA9, and

	Factor					
	SM	DM	OA	OM	IS	OP
SM1	0.388					
SM2	0.529					
SM3	0.583					
SM4	0.629					
SM5	0.560					
SM6	0.471					
DM1		0.648				
DM2		0.702				
DM3		0.662				
DM4		0.585				
DM5		0.615				
DM6		0.571				
DM7		0.640				
CS1			0.498			
CS2			0.571			
CS3			0.633			
CS4			0.522			
CS5			0.456			
CS6			0.313			
CS7			0.197			
CS8			0.299			
CS9			0.246			
OM1				0.251		
OM2				0.417		
OM3				0.747		
OM4				0.731		
OM5				0.730		
OM6				0.435		
IS1					0.652	
IS2					0.599	
IS3					0.613	
IS4					0.593	
IS5					0.589	
IS6					0.628	
IS7					0.607	
IS8					0.700	
IS9					0.599	
OP1						0.616
OP2						0.599
OP3						0.757
OP4						0.728
OP5						0.817
OP6						0.652

Note: Items with loadings less than 0.4 on their respective factor were shaded

Table III.
Simplified factor loading matrix

OM1 where loadings fell below the cutoff criterion. These variables, therefore, were excluded from subsequent analyses. As a result, the six-factor solution was confirmed and a distinct measurement model was defined for each latent factor: five-item sense-making (SM), seven-item decision-making (DM), five-item asset availability (OA), five-item operations management (OM), nine-item information security strategy implementation success (IS), and six-item organization performance (OP).

The measurement models were next estimated using confirmatory factor analysis to evaluate the construct internal reliability and validity prior to simultaneously estimating measurement and structural models. Internal reliability measures the consistency of items of the same construct, while validity measures the relations of the questionnaire items to the underlying constructs and the distinctiveness of different constructs (Warner, 2008). Internal reliability was assessed by computing a Cronbach's alpha reliability coefficient for each of the six constructs. Research literature suggested a reliability coefficient threshold of 0.70 indicating acceptable internal consistency (Hair *et al.*, 2006). It is found that all constructs' Cronbach α ranged from 0.869 to 0.934, demonstrating a high degree of internal reliability consistency. In SEM, convergent validity is tested by assuring *t*-value of 1.96 at the 0.05 level for all item loadings (Anderson and Gerbing, 1988; Schumacker and Lomax, 2004). As shown in Table IV, all items yielded standardized loadings statistically significant at $p < 0.05$ with *t*-tests > 1.96, indicating strong relations between the items and their corresponding constructs. Additionally, the item-to-total correlations were above 0.50, providing evidence of high convergent validity (Hair *et al.*, 2006). Table IV presents the final items and associated constructs, descriptive data for items, item-to-total correlations, standardized factor loadings and reliability coefficients for the constructs. Discriminant validity was confirmed by examining the pairwise factor variances in Table V, where average variance extracted for each construct were greater than the squares of the correlations between the construct and all other constructs (Fornell and Larcker, 1981). It is obvious that all values along the diagonal were greater than those in corresponding rows and columns, thus aiding in the determination for construct distinctiveness.

Finally, the six-measurement models were evaluated on multiple model fit criteria used in SEM to determine the fit between the hypothesized model and the observed data (McDonald and Ho, 2002). Although non-significant χ^2 is the traditional indicator for overall model fit, χ^2 is sensitive to sample size (Schumacker and Lomax, 2004; Kline, 2005; Reinard, 2006). Consequently, researchers have sought alternative model fit indices and have suggested the following acceptable threshold levels: the ratio of χ^2 and degree of freedom (df) < 5 (Bollen, 1989; Kline, 2005), the comparative fit index (CFI) and Tucker Lewis index (TLI) > 0.95, the standardized root mean square residual (SRMR) < 0.05 (Byrne, 2001), and the root mean square errors of approximation (RMSEA) < 0.08 (Hu and Bentler, 1999). Although all model fit statistics approached these levels, an examination of modification indices indicated that a better fit would be achieved if the error terms between the observed variables in the same constructs were free to correlate. After the correlated error terms were implemented, the modified measurement models were statistically superior compared to the original ones. Table VI presents the final model fit statistics for the measurement models. Overall, the confirmatory measurement models demonstrated good test results with acceptable internal reliability, convergent, and discriminant validity.

Construct	Observed variable	Mean	SD	Standardized estimate	*t*-test	Item-to-total correlation
SM	SM2	3.40	1.210	0.706[a]		0.654
$\alpha = 869$	SM3	3.99	1.012	0.844	15.771	0.742
	SM4	3.98	1.017	0.798	14.731	0.716
	SM5	3.81	1.064	0.759	14.073	0.703
	SM6	3.67	1.142	0.715	13.598	0.672
DM	DM1	3.50	1.100	0.806[a]		0.775
$\alpha = 934$	DM2	3.68	1.169	0.828	20.122	0.798
	DM3	3.33	1.216	0.818	19.566	0.788
	DM4	3.28	1.116	0.773	17.753	0.745
	DM5	3.30	1.176	0.819	19.165	0.788
	DM6	3.50	1.134	0.823	19.118	0.788
	DM7	3.25	1.165	0.859	20.496	0.823
OA	OA1	3.68	1.100	0.839[a]		0.791
$\alpha = 908$	OA2	3.57	1.154	0.784	18.781	0.733
	OA3	3.55	1.216	0.854	21.279	0.808
	OA4	3.66	1.085	0.832	20.471	0.788
	OA5	3.80	1.062	0.773	18.391	0.725
OM	OM2	3.31	1.094	0.655		0.647
$\alpha = 909$	OM3	3.13	1.156	0.91	16.058	0.847
	OM4	3.06	1.175	0.919	16.001	0.841
	OM5	3.10	1.178	0.886	15.678	0.832
	OM6	3.61	1.126	0.693	12.929	0.684
IS	IS1	3.91	0.985	0.823[a]		0.788
$\alpha = 932$	IS2	4.11	0.942	0.727	17.114	0.698
	IS3	3.89	0.990	0.797	19.447	0.768
	IS4	4.21	0.939	0.736	17.207	0.724
	IS5	4.03	0.912	0.672	15.152	0.655
	IS6	3.74	1.040	0.844	21.110	0.803
	IS7	4.09	0.958	0.729	16.840	0.704
	IS8	3.99	0.950	0.839	20.639	0.808
	IS9	3.70	0.953	0.823	19.972	0.776
OP	OP1	3.82	0.964	0.779[a]		0.744
$\alpha = 912$	OP2	3.92	0.923	0.741	16.176	0.708
	OP3	4.06	0.907	0.824	18.302	0.780
	OP4	3.85	0.952	0.807	17.746	0.756
	OP5	3.79	0.911	0.839	18.374	0.786
	OP6	3.92	0.938	0.788	17.280	0.749

Note: [a]Fixed parameter

Table IV.
Results of convergent validity and reliability analysis

	SM	DM	OA	OM	IS	OP
SM	*0.779*					
DM	0.631	*0.735*				
OA	0.680	0.705	*0.879*			
OM	0.477	0.499	0.530	*0.578*		
IS	0.559	0.554	0.642	0.450	*0.655*	
OP	0.389	0.386	0.447	0.313	0.456	*0.585*

Note: Average variance extracted was italicized and shown along the diagonal

Table V.
Construct correlations and discriminant validity analysis

5.3 Confirmatory structural model

A structural equation model encompassing the measurement models and structural model was established by extending the hypothesized relationships among the latent variables, depicted graphically with straight one-headed arrows as shown in Figure 2. According to the research hypotheses, organization performance was set as the dependent variable or endogenous latent variable. Information security strategy implementation success was also set as endogenous variable directly affecting organization performance. Four independent latent variables, sense-making, decision-making, asset availability, and operations management, were set as exogenous variables that had direct effects on information security strategy implementation success. The hypothesized structural equation model was tested using the maximum likelihood method and evaluated on the same fit criteria used in assessing the measurement models. Only the regression weight for

Model	χ^2	df	p	χ^2/df	SRMR	CFI	TLI	RMSEA
Acceptable fit thresholds				<5	≤ 0.05	≥ 95	≥ 95	<0.08
SM	9.941	3	0.019	3.314	0.0167	0.993	0.977	0.074
DM	27.622	11	0.004	2.511	0.0192	0.993	0.986	0.059
OA	1.756	2	0.416	0.878	0.0056	1.000	1.001	0.000
OM	7.046	3	0.070	2.349	0.0101	0.997	0.991	0.056
IS	59.238	21	0.000	2.821	0.0244	0.986	0.975	0.065
OP	19.412	7	0.007	2.773	0.0176	0.992	0.992	0.064

Table VI.
Fit indices for models in confirmatory measurement analysis

Notes: χ^2 – Chi-square; df – degrees of freedom; p – probability value; SRMR – standardized root; mean square residual; CFI – comparative fit index; TLI – Tucker Lewis index; RMSEA – root; mean square errors of approximation

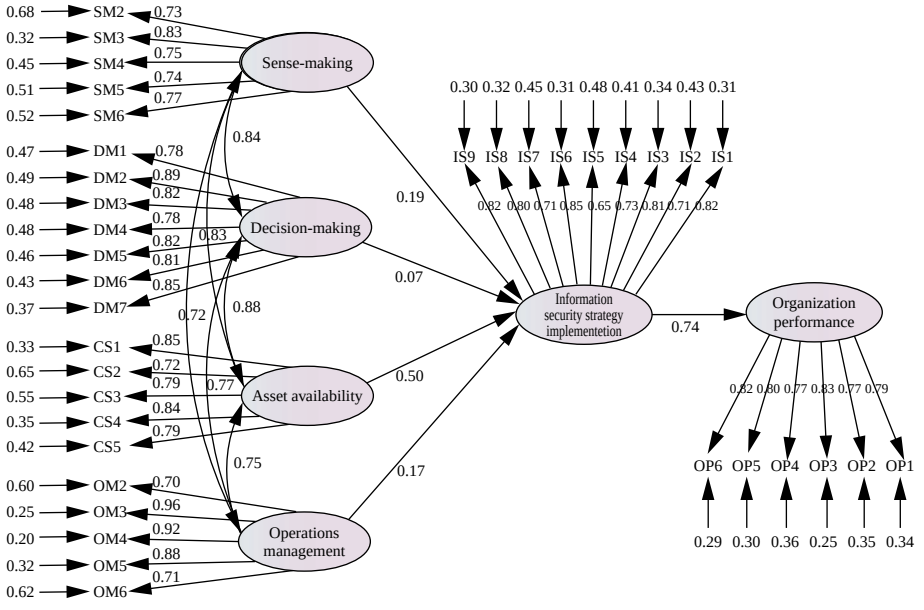

Figure 2.
Structural equation model

decision-making in the prediction of information security strategy implementation success is not significant at the 0.05 level. All other standardized path coefficients are significantly different from zero at the level of $p < 0.001$ and are shown in each arrow in Figure 2. The residual matrix is also shown in this figure. These values are small in magnitude and are not larger for one variable than another, indicating reasonable specification of the structural equation model (Schumacker and Lomax, 2004). The model χ^2 value is 1,069.1 with 600° of freedom, which is rather large and significant at $p = 0.000$. However, all alternative fit statistics in Table VII (χ^2/df = 1.782, SRMR = 0.0466, CFI = 0.963, TLI = 0.959, RMSEA = 0.043) exceed acceptable fit threshold levels, suggesting a good fit between the hypothesized model and the data. The model data confirms significant and positive associations between information security strategy implementation success and organization performance, sense-making, asset availability, operations management, respectively, at $p < 0.001$ (*H1*, *H2*, *H4*, and *H5* are supported). Of these hypothesized relationships, the path coefficient between information security strategy implementation success and organization performance is particularly greatest (0.74), followed by asset availability and information security strategy implementation success (0.50), sense-making and information security strategy implementation success (0.19), and then operations management and information security strategy implementation success (0.17). However, there is no significant correlation between decision-making and information security strategy implementation success at the level of $p < 0.05$ (*H3* is not supported). Note that there are strong correlations at the 0.001 level between decision-making and the remaining organizational capabilities discussed in this study. Of these relationships, the estimate is found particularly greatest with asset availability (0.88), followed by sense-making (0.84), and then operations management (0.77).

5.4 Standardized indirect effects

Table VIII reports the estimates of standardized direct effects, indirect effects, and total effects of organizational capability factors on organization performance. Proportional to the magnitude of the standardized direct effects of organizational capability factors on information security strategy implementation success, asset availability has the greatest standardized indirect effect on organization performance (0.372), followed by that of sense-making (0.141), then operations management (0.125). The results indicate that information security strategy implementation success mediates the relationships

χ^2	df	p	χ^2/df	SRMR	CFI	TLI	RMSEA
1,069.1	600	0.000	1.782	0.0466	0.963	0.959	0.043

Table VII.
Fit indices for structural equation model

Variable	Direct effects	Indirect effects	Total effects
Sense-making	0.000	0.141	0.141
Decision-making	0.000	0.049	0.049
Asset availability	0.000	0.372	0.372
Operations management	0.000	0.125	0.125

Table VIII.
Standardized effects of organizational capability factors on OP

between these three organizational capability factors and organization performance. Conversely, there is no significant indirect effect of decision-making on organization performance (0.049).

6. Discussion and conclusion

This study was designed to address the research questions concerning impacts of organizational capabilities on the effective implementation of information security strategy, and the relationship between information security strategy implementation success and organization performance. This was achieved by proposing and validating a theoretical model that demonstrates the linkage between information security strategy implementation effectiveness and organization performance, with organizational capabilities as key factors influencing the successful implementation of information security strategy. The research propositions asserted that essential organization capabilities must include developing high quality awareness and understandings of internal and external situations, making decisions with respect to planning and courses of action, obtaining and retaining appropriate skills and resources, as well as managing and measuring the information security program. These organization capabilities were represented in the model by the sense-making, decision-making, asset availability, and operations management variables. The model also consists of two additional variables, information security strategy sense-making, decision-making, asset availability, and operations management, encompassing six hypothesized constructs.

Based on existing literature in information security and strategic management, an original survey instrument was developed to collect empirical data. Using confirmatory factor analysis, the theoretical constructs were evaluated and evidence of acceptable internal reliability, convergent validity, and construct distinctiveness was assured. A SEM approach was utilized to quantitatively analyze data and to test the validity of the research hypothesis. SEM is a comprehensive statistical technique for testing hypothesis and fitting the structural equation model, taking into account observed and latent variables as well as measurement error terms (Schumacker and Lomax, 2004). Although χ^2 is the traditional measure used in assessing overall model fit, it tends to be unreliable when sample sizes larger than 200 are used (Reinard, 2006). Researchers suggested that alternative fit indexes be used as there is no agreement on the best single approach for evaluating model fits. Amid the large sample size used in this study (428), alternative fit tests including χ^2/df, SRMR, CFI, TLI, RMSEA were reported. In the hypothesized model, all fit statistics exceed the thresholds for acceptable fit, indicating a good fit between sample data and the theoretical patterns in the data.

The results of this study contribute to existing literature for the knowledge of organizational capability factors consisting of sense-making, asset availability and operations management, that have direct effects on the effective implementation of information security strategy and indirect effects on organization performance. Of the organizational capabilities surveyed, the asset availability factor, reflecting the extent to which an organization is able to obtain and organize the competencies, resources, and processes needed to accomplish information security strategy goals, is the most critical organizational capability in the model. Next to asset availability, sense-making is the second most essential capability, then operations management. Furthermore, information security strategy implementation success is confirmed to have a positive association with organization performance and mediate the relationships between the three organizational

capabilities and organization performance. However, the research did not find a significant correlation between decision-making and information security strategy implementation success. On the other hand, the results showed strong correlations between decision-making and other organizational capabilities, namely sense-making, asset availability, and operations management. It is recommended that further research be pursued to achieve a definitive conclusion on the role of decision-making in information security.

Two possible limitations and ensuing recommendations for future research were identified in this study. First, the survey instrument was perceived as designed with focus on medium-to-large firms in the private sector. Future use of this instrument may benefit from higher response rates if the organization performance scale is revised to better apply to government/non-profit organizations. For example, a research participant stated that "There is no business value for a government agency. There are compliance requirements, but no real penalties for non-compliance." Follow-on studies are recommended to examine the moderating effects of the size and type of organizations on the association between organizational capabilities and information security strategy implementation. Second, there may be a potential source of bias resulting from the technical nature of the intended population. By polling primarily information security specialists, the results may have been partially influenced by their inherently technical perspective. For greater generalizability of the results, the targeted sample should exemplify a reasonable mix of information security professionals and individuals in managerial and strategic planning positions. In today's environment, information security is increasingly seen as a business driver, which concept reflects the need for involvement and support at the board and executive levels and throughout the organization. Thus, to further the generalized knowledge of the impacts of organizational capabilities in information security, the recommendation to incorporate a higher percentage of senior managers and executives in the respondent sample is worth investigation.

The results of this study have several business implications. By analyzing an organization's information security capabilities as an aggregation of sense-making, decision-making, asset availability, and operations management, this study provides business an understanding of and insight into the viable predisposition of organizational capabilities in the context of information security. Evidence of organizational capabilities' positive effects on information security strategy and organization performance highlights the importance and consequence of an organization's intangible assets as it competes in today's challenging marketplace. Business leaders should focus on organizational capabilities that provide high valued contributions to the accomplishment of information security strategy goals and organizational objectives, enabling their businesses to achieve market-leading performance and thus competitive advantage.

References

Alberts, D. (2003), *Information Age Transformation: Getting to a 21st Century Military*, CCRP Publication, Washington, DC.

Alberts, D. and Hayes, R.E. (2003), *Power to the Edge: Command, Control in the Information Age*, CCRP Publication, Washington, DC.

Alberts, D., Garstka, J.J., Hayes, R.E. and Signori, D.T. (2001), *Understanding Information Age Warfare*, CCRP Publication, Washington, DC.

Allen, J. (2005), *Governing for Enterprise Security*, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, available at: www.sei.cmu.edu/reports/05tn023.pdf (accessed 11 February 2010).

Amaio, T.E. (2009), "Exploring and examining the business value of information security: corporate executives' perceptions", PhD diss., Northcentral University, Prescott, AZ.

Anderson, E. and Choobineh, J. (2008), "Enterprise information security strategies", *Computers and Security*, Vol. 27 Nos 1-2, pp. 22-9.

Anderson, J.C. and Gerbing, D.W. (1988), "Structural equation modeling in practice: a review and recommended two-step approach", *Psychological Bulletin*, Vol. 103 No. 3, pp. 411-23.

Ansoff, I. (1965), *Corporate Strategy*, Penguin Books, New York, NY.

Barney, J. (1991), "Firm resources and sustained competitive advantage", *Journal of Management*, Vol. 17 No. 1, pp. 99-120.

Barney, J.B. and Zajac, E.J. (1994), "Competitive organizational behavior: of competitive advantage", *Strategic Management Journal*, Vol. 15, S1, pp. 5-9.

Bollen, K.A. (1989), *Structural Equations with Latent Variables*, Wiley, New York, NY.

Bourque, L.B. and Fielder, E.P. (2003), *How to Conduct Self-Administered and Mail Survey*, 2nd ed., Sage Publications, Thousand Oaks, CA.

Byrne, B. (2001), *Structural Equation Modeling with Amos: Basic Concepts, Applications, and Programming*, Lawrence Erlbaum Associates, Mahwah, NJ.

Caralli, R.A. (2004), *Managing for Enterprise Security*, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, available at: www.sei.cmu.edu/reports/04tn046.pdf (accessed 11 February 2010).

Chang, S.E. and Ho, C.B. (2006), "Organizational factors to the effectiveness of implementing information security management", *Industrial Management & Data Systems*, Vol. 106 No. 3, pp. 345-61.

Cockburn, I.M., Henderson, R.M. and Stern, S. (2000), "Untangling the origins of competitive advantage", *Strategic Management Journal*, Vol. 21 Nos 10/11, pp. 1123-45.

Collis, D.J. (1994), "How valuable are organizational capabilities?", *Strategic Management Journal*, Vol. 15, pp. 143-52.

Deloitte (2008), "Gaining momentum: the 2008 energy & resources global security survey", available at: www.deloitte.com/assets/Dcom-Turkey/LocalAssets/Documents/Turkey-En_ers_ER-SecuritySurvey_220808.pdf (accessed 28 October 2010).

Eisenhardt, K.M. and Martin, J.A. (2000), "Dynamic capabilities: what are they?", *Strategic Management Journal*, Vol. 21 Nos 10-11, pp. 1105-21.

Ernst & Young (2007), "Ernst & Young 2007's global information security survey", available at: www2.eycom.ch/publications/items/2007_giss/2007_ey_giss.pdf (accessed 28 October 2010).

Ernst & Young (2008), "Ernst & Young 2008's global information security survey", available at: www.ey.com/Publication/vwLUAssets/GISS_2008/$FILE/GISS2008.pdf (accessed 28 October 2010).

Ezingeard, J., McFadzean, E. and Birchall, D. (2005), "A model of information assurance benefits", *Information Systems Management*, Vol. 22 No. 2, pp. 20-9.

FFIEC (2006), *Information Security Booklet*, available at: www.ffiec.gov/ffiecinfobase/booklets/information_security/information_security.pdf (accessed 28 October 2010).

Fornell, C. and Larcker, D.F. (1981), "Evaluating structural equation models with unobservable variables and measurement error", *Journal of Marketing Research*, Vol. 18 No. 1, pp. 39-50.

Fratto, M. (2009), "2009 strategic security survey", available at: http://i.cmpnet.com/custom/strategicsecurity/assets/InformationWeek_Analytics_2009_Strategic_Security_Survey.pdf (accessed 28 October 2010).

Gold, A.H., Malhotra, A. and Segars, A.H. (2001), "Knowledge management: an organizational capabilities perspective", *Journal of Management Information Systems*, Vol. 18 No. 1, pp. 185-212.

Grant, R.M. (1991), "The resource-based theory of competitive advantage: implications for strategy formulation", *California Management Review*, Vol. 33 No. 3, pp. 114-35.

Hair, J., Tatham, R.L., Anderson, R.E. and Black, W. (2006), *Multivariate Data Analysis*, 6th ed., Pearson Prentice-Hall, Upper Saddle River, NJ.

Hu, L. and Bentler, P.M. (1999), "Cutoff criteria for fit indexes in covariance structure analysis' conventional criteria versus new alternatives", *Structural Equation Modeling*, Vol. 6 No. 1, pp. 1-55.

Huang, C.D. and Hu, Q. (2007), "Achieving IT-business strategic alignment via enterprise-wide implementation of balanced scorecards", *Information Systems Management*, Vol. 24 No. 2, pp. 173-84.

ISACA (2009), "An introduction to the business model for information security", available at: www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/An-Introduction-to-the-Business-Model-for-Information-Security.aspx (accessed 28 October 2010).

Kankanhalli, A., Teo, H., Tan, B.C.Y. and Wei, K. (2003), "An integrative study of information systems security effectiveness", *International Journal of Information Management*, Vol. 23 No. 2, pp. 139-54.

Kaplan, R.S. and Norton, D.P. (2007), "Using the balanced scorecard as a strategic management system", *Harvard Business Review*, Vol. 85 Nos 7/8, pp. 150-61.

Kelly, D. and Amburgey, T.L. (1991), "Organizational inertia and momentum", *The Academy of Management Journal*, Vol. 34 No. 3, pp. 591-612.

Kim, G. (2004), "Does security set the right goals?", *Security Management*, Vol. 48 No. 6, p. 182.

Kline, R. (2005), *Principles and Practice of Structural Equation Modeling*, 2nd ed., Guilford, New York, NY.

Knapp, K.J., Marshall, T.E., Rainer, R.K. and Ford, F.N. (2006), "Information security: management's effect on culture and policy", *Information Management & Computer Security*, Vol. 14 No. 1, pp. 24-36.

Kusunoki, K., Nonaka, I. and Nagata, A. (1998), "Organizational capabilities in product development of Japanese firms: a conceptual framework and empirical findings", *Organization Science*, Vol. 9 No. 6, pp. 699-718.

McDonald, R.P. and Ho, M.R. (2002), "Principles and practice in reporting structural equation analyses", *Psychological Methods*, Vol. 7 No. 1, pp. 64-82.

McFadzean, E., Ezingeard, J. and Birchall, D. (2007), "Perception of risk and the strategic impact of existing IT on information security strategy at board level", *Online Information Review*, Vol. 31 No. 5, pp. 622-60.

NIST (2007), *Information Security Guide for Government Executives*, available at: http://csrc.nist.gov/publications/nistir/ir7359/NISTIR-7359.pdf (accessed 28 October 2010).

NIST (2008), *Draft NIST Special Publication 800-39, Information Security – Managing Risk from Information Systems: An Organizational Perspective*, available at: http://csrc.nist.gov/publications/drafts/800-39/SP800-39-spd-sz.pdf (accessed 28 October 2010).

Nyanchama, M. (2005), "Enterprise vulnerability management and its role in information security management", *Information Systems Security*, Vol. 14 No. 3, pp. 29-56.

Park, S. and Ruighaver, T. (2008), "Strategic approach to information security in organizations", paper presented at the 2008 International Conference on Information Science and Security, IEEE Computer Society, Seoul, Korea.

Porter, M. (1985), *Competitive Advantage: Creating and Sustaining Superior Performance*, The Free Press, New York, NY.

Prahalad, C. and Hamel, G. (1990), "The core competence of the corporation", *Harvard Business Review*, pp. 79-91.

PricewaterhouseCoopers (2008), "PWC global state of information security survey 2008 – improving security: an action plan", available at: www.pwc.com/gx/en/information-security-survey/index.jhtml (accessed 28 October 2010).

Rangone, A. (1999), "A resource-based approach to strategy analysis in small-medium sized enterprises", *Small Business Economics*, Vol. 12, pp. 223-48.

Rathnam, R.G., Johnsen, J. and Wen, H.J. (2004), "Alignment of business strategy and it strategy: a case study of a Fortune 500", *The Journal of Computer Information Systems*, Vol. 45 No. 2, pp. 1-8.

Reinard, J. (2006), *Communication Research Statistics*, Sage, Thousand Oaks, CA.

Saugatuck Technology (2008), "Enterprise information management for competitive advantage", available at: www.synaptica.com/djcs/synaptica/Enterprise%20Information%20Mgmt_DJWhitepaper033108.pdf (accessed 28 October 2010).

Schultz, E. (2006), "The changing winds of information security", *Computers and Security*, Vol. 25 No. 5, pp. 315-6.

Schumacker, R.E. and Lomax, R.G. (2004), *A Beginner's Guide to Structural Equation Modeling*, 2nd ed., Lawrence Erlbaum Associates, Mahwah, NJ.

Slater, S.F. and Olson, E.M. (2001), "Marketing's contribution to the implementation of business strategy: an empirical analysis", *Strategic Management Journal*, Vol. 22 No. 11, pp. 1055-67.

Smallwood, N. and Panowyk, M. (2005), "Building capabilities", *Leadership Excellence*, Vol. 22 No. 1, p. 17.

Stalk, G., Evans, P. and Shuman, L.E. (1992), "Competing on capabilities: the new rules of corporate strategy", *Harvard Business Review*, Vol. 70 No. 2, pp. 54-66.

Straub, D.W. and Effective, I.S. (1990), "Security: an empirical study", *Information Systems Research*, Vol. 1 No. 3, pp. 255-76.

Symantec (2009), "Symantec internet security threat report trends for 2008", available at: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf (accessed 28 October 2010).

Tallon, P.P., Kraemer, K.L. and Gurbaxani, V. (2000), "Executives' perceptions of the business value of information technology: a process-oriented approach", *Journal of Management Information Systems*, Vol. 16 No. 4, pp. 145-73.

TechAmerica (2009), "Nineteenth annual survey of federal chief information officers", available at: www.techamerica.org/techamerica-and-grant-thornton-release-19th-annual-survey-of-federal-cios (accessed 28 October 2010).

Teece, D.J., Pisano, G. and Shuen, A. (1997), "Dynamic capabilities and strategic management", *Strategic Management Journal*, Vol. 18 No. 7, pp. 509-33.

Ulrich, D. and Lake, D. (1991), "Organizational capability: creating competitive advantage", *Academy of Management Executive*, Vol. 5 No. 1, pp. 77-92.

Ulrich, D. and Smallwood, N. (2004), "Capitalizing on capabilities", *Harvard Business Review*, Vol. 82 No. 6, pp. 119-27.

van Opstal, D. and Council on Competitiveness (2007), "The resilient economy: integrating competitiveness and security, council on competitiveness", available at: www.compete.org/images/uploads/File/PDF/Files/Transform_The_Resilient_Economy_FINAL_pdf.pdf (accessed 28 October 2010).

von Solms, B. (2006), "Information security – the fourth wave", *Computers and Security*, Vol. 25 No. 3, pp. 165-8.

Warner, R. (2008), *Applied Statistics: From Bivariate Through Multivariate Techniques*, Sage, Los Angeles.

Werlinger, R., Hawkey, K. and Beznosov, K. (2009), "An integrated view of human, organizational, and technological challenges of it security management", *Information Management & Computer Security*, Vol. 17 No. 1, pp. 4-19.

Wernerfelt, B. (1984), "A resource-based view of the firm", *Strategic Management Journal*, pp. 171-80.

Wethyavivorn, P., Charoenngam, C. and Teerajetgul, W. (2009), "Strategic assets driving organizational capabilities of Thai construction firms", *Journal of Construction Engineering and Management*, Vol. 135 No. 11, pp. 1222-31.

Wood, C.C. (1993), "Achieving competitive advantage with information security", *Managerial Auditing Journal*, Vol. 8 No. 2, pp. i-iv.

Further reading

Bennett, J.A. (2000), "Focus on research methods mediator and moderator variables in nursing research: conceptual and statistical differences", *Research in Nursing & Health*, No. 23, pp. 415-20.

Hall, J., Sarkani, S. and Mazzuchi, T.A. (2010), "Moderating roles of organizational capabilities in information security", paper presented at the 5th International Conference on i-Warfare & Security (ICIW 2010), Dayton, Ohio, 8-9 April.

Klein, A. (2007), "Building an identity management infrastructure for today and tomorrow", *Information Systems Security*, Vol. 16, pp. 74-9.

Lattin, J., Carroll, J.D. and Green, P.E. (2003), *Analyzing Multivariate Data*, Brooks Cole, Pacific Grove, CA.

About the authors

Jacqueline H. Hall is currently a Doctoral Student in Engineering Management and Systems Engineering at The George Washington University. She received a BS (1990) in Electrical Engineering and an MBA (1998) in Information Systems from Old Dominion University, and an MS (2009) in Systems Engineering from the George Washington University. Jacqueline H. Hall is the corresponding author and can be contacted at: halljj_98@yahoo.com

Shahram Sarkani, PhD, PE, is a Professor of Engineering Management and Systems Engineering at The George Washington University. Professor Sarkani joined the GW faculty in 1986, where his administrative appointments include Chair of the Civil, Mechanical, and Environmental Engineering Department (1994-1997); School of Engineering and Applied Science Interim Associate Dean for Research and Development (1997-2001); and Faculty Adviser, Academic Director and Head of EMSE Off-Campus Programs (since 2001). In his current role, Professor Sarkani designs and administers off-campus programs on behalf of the Department of Engineering Management and Systems Engineering. Today EMSE-OCP offers classes in over 25 cities around the USA and overseas, and enrolls about 1,200 graduate students pursuing Master's and Doctoral degrees in Systems Engineering and in Engineering Management.

Professor Sarkani holds a PhD in Civil Engineering from Rice University, and BS and MS degrees in Civil Engineering from Louisiana State University. He is a Registered Professional Engineer.

Thomas A. Mazzuchi received a BA (1978) in Mathematics from Gettysberg College, Gettysberg, PA, a MS (1979) and a DSc (1982), both in Operations Research from the George Washington University, Washington, DC. Currently, he is a Professor of Engineering Management and Systems Engineering in the School of Engineering and Applied Science at the George Washington University, Washington, DC. He is also the Chair of the Department of Engineering Management and Systems Engineering at the George Washington University, where he has served as the Chair of the Operations Research Department and as Interim Dean of the School of Engineering and Applied Science. Dr Mazzuchi's current research interests include reliability growth assessment, software reliability modeling, design and inference in life testing, reliability estimation as a function of operating environment, maintenance inspection policies, and incorporation of expert judgment into reliability and risk analysis.