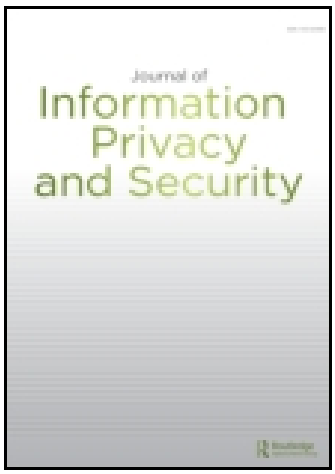


Journal of Information Privacy and Security
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/uips20

Acquiring Subject Participation for Information Security Survey Research: A Content and Correspondence Analysis Approach

Alice M. Johnson & Belinda P. Shipps
Published online: 07 Jul 2014.

To cite this article: Alice M. Johnson & Belinda P. Shipps (2013) Acquiring Subject Participation for Information Security Survey Research: A Content and Correspondence Analysis Approach, Journal of Information Privacy and Security, 9:4, 3-30, DOI: 10.1080/15536548.2013.10845688

To link to this article: http://dx.doi.org/10.1080/15536548.2013.10845688

Acquiring Subject Participation for Information Security Survey Research: A Content and Correspondence Analysis Approach

Alice M. Johnson (corresponding author), Department of Business Administration College of Business and Economics, North Carolina A&T State University, 1601 E. Market St., Greensboro, NC 27411, Phone: 336-285-3394 and Fax: 336-256-2645, E-mail: amjohns1@ncat.edu

Belinda P. Shipps, Department of Business Administration, College of Business and Economics, North Carolina A&T State University, 1601 E. Market St., Greensboro, NC 27411, Phone: 336-285-3358 and Fax: 336-256-2645, E-mail: bpshipps@ncat.edu

ABSTRACT

Twenty-four business executives and 22 security executives had previously participated in a study about information security investment. The current study asked participants to comment on their reasons for participating in that research. A total of 1003 reasons were submitted which were used to perform a content analysis of information security survey research (ISSR) participation factors. Security and business executives' reasons for participating differed. Reasons also differed by industry. The findings will help researchers to properly communicate the benefits of their studies and thus increase participation rates for ISSR. Greater participation will perhaps contribute to efforts to improve information security.

KEYWORDS

Information security survey research; information security executive; business executive; content and correspondence analysis

INTRODUCTION

The importance of information security is evident because it has been on the top 10 list of management concerns each year since 2003 (Luftman and Derksen 2012). Moreover, funding for information security has continued to increase relative to the overall information technology (IT) budget (CSI 2010/2011). Although managers have acknowledged the importance of information security, few will agree to engage in survey research to address the issue. Some reasons cited for such hesitancy are job security concerns, absence of a formal information security program, and the sensitivity of the information (Kotulic and Clark 2004).

Previous studies have identified a number of factors that encourage participation in survey research in general (e.g., Dillman 2000; Maynard et al. 2010; Schleifer 1986) as well as participation in surveys for specific contexts (e.g., Halpern et al. 2004; Sanginga et al. 2006). Although previous information security survey research (ISSR) has employed the practices suggested by those studies, researchers have experienced difficulty acquiring respondents. For example, a recent Computer Crime and Security Survey reported that fewer respondents than ever were willing to share specific information (CSI 2010/2011). Also, in spite of rigorous efforts to obtain subjects for a survey to validate a proposed information security model, Kotulic and Clark (2004) were unable to do so because of a low response rate. As a result they addressed the issue, "why there aren't more information security research studies" (p. 597) and answered the question by identifying reasons why organizations refused to participate. However, previous studies have not investigated factors that might motivate organizations *to participate* in ISSR. The current research fills that gap. Information security surveys are different from other research because they address very sensitive subjects for organizations and are one of the most intrusive types of research where there is a general mistrust of any external entity that might attempt to obtain data about the firm's information security activities (Kotulic and Clark 2004). Such mistrust would inhibit participation in ISSR. Therefore, it is reasonable to expect that the mere application of survey participation factors in other contexts might not be appropriate for ISSR.

Knowledge about factors that motivate participation might result in more information security survey studies and hence improvements in methods to secure organizational information. Better security would help to prevent security breaches and thus positively contribute to organizational performance by reducing the financial losses incurred as a result of such breaches. A recent survey found that 41.1% of the respondents had experienced a security incident within a given year (CSI 2011/2012). The current research was initiated to elucidate factors that might motivate individuals to participate in ISSR. It is reasonable to expect that security and business managers might be motivated by different factors (Ranier et al. 2007; Tai and Phelps 2000). Further, research has consistently shown that study results are affected by industry (Hrebiniak and Snow 1980). Therefore, the current study investigates the following questions:

Q1: What are the factors that motivate subjects to participate in information security survey research?

Q2: Do business and security subjects' reasons for participation in information security survey research differ?

Q3: Does industry type influence the reasons subjects agree to participate in information security survey research?

An objective of the study was to provide an understanding of factors that motivate one to participate in ISSR. Considering that little was known *a priori* about such

participation, our study was exploratory and we chose to use grounded theory techniques that would permit the discovery of theory in lieu of the prediction of outcomes. Therefore, in accordance with grounded theory, we did not specify hypotheses. However, we used a variety of methods to collect data (both qualitative and quantitative) which would be the basis for the creation of a theory about ISSR participation (Allan 2003).

BACKGROUND

Information Security Research

The Federal Information Security Management Act of 2002 (FISMA) has stated that information security means "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide integrity, confidentiality, and availability" (csrc.nist.gov, p. 49). Because of the widespread use of information systems and the occurrence of legislation that governs the use and protection of data stored in digital format, research about information security has become increasingly important. However, the literature on information security is fragmented primarily because of the limited number of interdisciplinary studies (Siponen and Oinas-Kukkonen 2007). Previous research has focused on broad areas of study such as information security management, user behavior, access controls, and information security best practices.

Information security management (ISM) studies include the investigation of planning tasks that help to ensure business continuity as well as effective backup and recovery of an organization's information systems. Ideally, ISM activities should be aligned with business objectives. Moreover, documentation should exist to elucidate how those activities support the organization's mission ((Siponen and Oinas-Kukkonen 2007).

Although an organization may implement acceptable information security policies and plans, ultimately the firm must rely on its employees to ensure success. Thus, users' behaviors are an important element regarding information security. Moreover, a user's information processing mode influences their intention to comply with security recommendations. Individuals who process information symmetrically are more likely to comply, whereas those who do not make much effort to process it are less likely to do so (Zhang and Amos 2012). A conceptual model identified six factors that influenced user behavior (Leach 2007). They were (1) what employees (i.e., users) are told within the firm about information security, (2) users' personal values and standards of conduct, (3) psychological contract with the organization, (4) the effort required to comply and temptations not to comply, (5) the user's security common sense and decision making skills, and (6) behaviors demonstrated by senior management and colleagues. Because a firm's primary objective is to decrease the number of security incidences, Leach's (2007) model proposes that this objective could be achieved by manipulating the six user security behaviors. Drawing on the model, Abraham (2011) conducted a critical analysis of articles about information

security behavior. That study resulted in 18 themes for security practitioners and researchers to consider for information security implementations.

Spears and Barki (2010) also studied the role of the user in protecting information systems assets. More specifically, they examined user participation in information systems security risk management activities and found that such participation helped to increase awareness about information security and thus provided better protection for sensitive information in business processes. However, a primary obstacle to awareness is due more to the application of security knowledge than the lack of such knowledge (Slusky and Partow-Navid 2012).

Studies about access controls have addressed specific activities required to protect sensitive data stored in digital format. The objective is to ensure that the provisions of integrity, availability, and confidentiality, as outlined in FISMA, are not compromised. An important contribution in this area of information security research is advancements in methods of authentication such as the use of passwords (Denning 1992), smart cards (Lambrinoudakis 2000), and biometrics (Venkatraman and Delpachitra 2008). Additionally, researchers have examined access control for Internet-based information systems (Diaz et al. 1998).

Researchers as well as other professionals have proposed a number of best practice frameworks to facilitate organizations efforts to effectively implement information security programs. Examples of such frameworks are Control Objectives for Information and Related Technology (COBIT), International Organization for Standardization / International Electrotechnical Commission 17799 (ISO/IEC 17799), Information Technology Infrastructure Library (ITIL), and Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) standards. Refer to Saint-Germain (2005) for a thorough analysis of these as well as other information security best practices frameworks.

The ISO/IEC 17799 has provided a variety of procedures that could be adopted by organizations to help ensure its information systems assets. It is more comprehensive than the other frameworks.

> ISO/IEC 17799 comprises 10 security domains and seeks to address security compliance at all levels: managerial, organizational, legal, operational, and technical. It includes 36 control objectives, consisting of general statements of security goals for each of the 10 domains. The standard also includes 127 controls that identify specific means for meeting the control objectives. Organizations implement these controls to mitigate the risks they have identified. (Saint-Germain 2005, p 61).

A recent study confirmed the comprehensiveness of the ISO/IEC 17799 standard. However, that same study also provided a more parsimonious eight factor model (Ma and Pearson 2005).

Kotulic and Clark (2004) proposed a conceptual model that would assess the effectiveness of a firm's information security practices. Their model proposed that executive management support, the actual performance of the implemented practices (in terms of the level and cost of the security breach), and the difference between desired and actual performance would influence the effectiveness of information security practices. However, after engaging in diligent data collection activities, their efforts resulted in an "extremely poor response rate" (p. 604) for their survey. Therefore, they were unable to test the model. However, an unexpected contribution of their research was information obtained from potential respondents about their reasons for not participating in the survey.

Research Participation

Literature that specifically addresses factors that inhibit or promote participation in ISSR is sparse. However, studies have suggested that the sensitivity of the information shared, the benefit versus the cost of participating, top management support, and the absence of a formal security program are inhibitors, whereas the initial development of positive relationships with prospective subjects/firms is a facilitator (Kotulic and Clark 2004). The factors that influence a potential respondent's decision to participate in research, in general, are dynamic. Much has been written about the topic. One stream of research has presented analytical models that delineated participation factors, while another stream has provided empirical studies that focused on participation for specific fields of interest.

Groves and Couper (1998) proposed a conceptual framework of survey participation which posited that researchers could acquire participation by customizing the request to the concerns of the potential subject. Using a technique referred to as tailoring, the premise is that the researcher would increase the salience of features that would most likely appeal to the participant. Drawing on the concept of tailoring, the leverage-saliency theory of survey participation suggests that a single research design attribute might result in an affirmative decision to participate for different prospective respondents (Groves et al. 2000). Moreover, it posits that a potential subject has an expected utility associated with participating in a research project. Hence, the subject will agree to participate if the expected utility surpasses that of other uses of time and effort (Roose et al. 2007).

A recent framework indicated that a respondent's decision to participate in research resulted from external factors that were outside the researcher's control as well as internal factors that could perhaps be controlled by the researcher (Groves and Couper1998). External factors included individual differences of the potential respondents and environmental conditions (e.g., economic conditions and survey-taking climate). Internal factors included the survey design and researcher characteristics.

Previous research has confirmed the conceptual frameworks of participation by addressing issues about such participation for specific areas of interest. For example,

an early study conducted by the U.S. Census Bureau found that the length of the confidentiality assurance provided to potential respondents influenced participation. One fifth of the potential respondents were assured confidentiality forever, one fifth for 75 years, one fifth for 25 years, one fifth receive no assurance of confidentiality, and the final fifth were told their responses would be available to the public. The rate of no-participation increased with decreasing rates of confidentiality assurance (National Research Council 1979)

Halpern et al. (2004) studied the effect of providing incentives for participation in clinical trial research. They found that participation in such research increased when financial incentives were provided. Willingness to participate was directly related to the amount of the payment. Furthermore, a higher financial incentive was required to obtain participation from respondents with a higher income.

Another study provided strategies for procuring subject participation in health research. It focused specifically on the challenge of obtaining participation from low-income Latinos for health research projects. The researchers tailored their scripts and approaches for requesting participation depending on the gender of the potential respondent. They found that men participated in the research to gain knowledge, whereas females participated because they wanted to help the researcher (Preloran et al.2001).

Factors that influence participation in agricultural research have also been investigated. Five such factors emerged from one study. They were gender, household size, contact with external services, location of residence, and decision–making pattern. More specifically, females had a higher probability of participation, as did individuals from households where a cooperative and bargaining decision-making pattern existed (Sanginga et al. 2006). Table 1 provides a summary of participation factors identified in previous research.

Table 1. Research Participation Factors Identified in Previous Studies

Factor	Author(s)
Frequency of past participation	Schleifer 1986
Perceived legitimacy of the research	Schleifer 1986
Research design	Schleifer 1986 Chesney 2006
Survey topic	Steeh 1981 Roose et al. 2007 Galea and Tracey 2007 Groves et al. 2004
Researcher characteristics	Singer and Kohnke-Aguirre 1979 Oksenberg et al. 1986 Schleifer 1986
Consistent with existing values and commitments	Groves et al. 1992
Feelings of obligation	Groves et al. 1992
Wanted my opinion to be counted	Groves et al. 1992
Incentive(s) provided by the researcher	Groves et al. 1992
Perceived legitimacy of a sponsor	Groves et al. 2000 Groves et al. 2004
Worthy of participant's time and effort	Maynard et al. 2010
Saturation of requests to participate Overall decrease in volunteerism	Galea and Tracey 2007

METHODOLOGY

The Participants

The subjects had recently participated in a study about information security investment (Johnson 2009). Each was asked to share their reasons for participating in that study. Forty-six subjects (i.e., 24 business executives and 22 security executives) agreed to do so. Thus, 100% of the solicited subjects agreed to participate. Thirty-three companies and 13 industries were represented. Table 2 summarizes the demographics and characteristics of the participants.

Table 2.Demographics and Characteristics of Participants

	Number of Subjects		
Industry	**Business**	**Security**	**Number of Employees**
Education	2	2	17,310
Entertainment	2	2	2,700
Finance	3	1	351,400
Government	2	3	11,000
Healthcare	3	4	35,400
Insurance	1	1	15,000
Manufacturing	1	1	95,000
Publishing	2	2	1,600
Real Estate	1	2	80,370
Restaurant	1	1	5,000
Retail	2	1	466,500
Transportation	2	0	130,000
Utilities	2	2	20,000

The 33 organizations had an average gross revenue of $9.4 billion and average profit or net income was $991 million. Business executives had an average of 34 years industry experience, 22 years with their organization, and 17 years in their position with their organization. The CEO title was held by twenty of the business executives while the other 4 had titles consistent with the highest business executive in the organization. Approximately 67% of the business executives had engaged in postgraduate work and 8% had postgraduate degrees.

Security executives had an average of 18 years industry experience, 12 years with the organization, and 9 years in the information security position with their organization. Each was responsible for managing their firm's information security function. One reported directly to the organization's financial administrator, three reported to the organization's chief auditor, and the remaining 18 reported directly to the top information systems executive. Twenty-four percent of them had participated in postgraduate work and another 24% had postgraduate degrees.

Data Collection

Three phases were used to collect the data. The instruments used in each phase are contained in the Appendix. First, each participant received via postal mail a survey package. It contained a document that asked each to indicate their reasons for participating in the previous information security investment study, an electronic link address where the responses could be submitted online, and a pre-paid envelope for those who preferred to use the document for their responses and return it through postal mail. Respondents were encouraged to list at least 10 reasons. Twenty-one of the responses were received within two weeks of the mailing date of the package. Another 16 responded within three weeks. If a response was not received within three weeks, the non-respondent was contacted via email and telephone to further solicit participation. After five weeks, all responses were received.

A total of 1003 participation reasons were submitted. Table 3 shows a breakdown of the most and least reasons submitted by a single participant and the average number of reasons submitted for each subject category.

Table 3. Number of Reasons for Participation

	Business	**Security**
Most submitted by a single participant	34	30
Least submitted by a single participant	15	10
Average number submitted	23	21
Total number submitted	551	452

The 1003 responses would be used as input to a content analysis of participation reasons. Content analysis has been widely used in research to study and explain communication by "analyzing data with a specific context in view of the meanings someone – a group or a culture – attributes to them." (Krippendorff 1980, p. 403). Its objective is to transform documented text into reliable information that can be used for future reference.

Three information systems professors served as coders for the content analysis. Literature had indicated that a variety of factors influenced participation in survey research. However, as indicated by Kotulic and Clark (2004), procuring such participation for ISSR had special challenges that were not existent in other types of research. Moreover, research to address participation factors for ISSR was limited. Thus, it was appropriate to pursue a conventional content analysis for the current study where preconceived categories were not employed. Instead researchers studied the data intensely and permitted the categories to emerge from the data. This method is also referred to as inductive category development (Mayring 2000).

Methods suggested by Moore and Benbasat (2001) were largely used to guide the efficacy of the content analysis and thus assess construct validity. Each coder

independently reviewed the 1003 responses multiple times to capture the key themes or concepts. Notes were taken and keywords were highlighted. The keywords were used to define and label the categories/constructs. Subsequent to the completion of the individual analysis, the Cohen Kappa (K) statistic (Cohen 1960) was used to measure pairwise agreement among the coders for the constructs. K ranged from .81 to .90, thus indicating acceptable interrater reliability (Krippendorff 1980). If coders could not agree on the interpretation of a response, the subject was contacted for clarification.

After determining the exact wording of the construct labels, each coder sorted the 1003 items into the categories independent of the other coders. Interrater reliability for each construct was assessed. Kappa scores ranged from .85 to .96. As suggested by Moore and Benbasat (2001), convergent and discriminant validity was also assessed. Generally, items consistently placed within the same specific category among the three judges. Such placement suggested convergent validity with the assigned construct as well as discriminant validity with the others.

The second phase of data collection provided subjects with a list of 33 participation reasons that were discovered from the content analysis data that was done in phase one. Each subject indicated on a scale of 1 (no extent) to 5 (great extent) the extent to which the item influenced their decision to participate in the research. One other scaled item asked each respondent to rate the extent to which his/her participation had benefited their organization.

The third phase of data collection included semi-structured interviews which were employed to further elucidate the respondents' reasons for participating in the study and their perceived benefits of doing so. Following the recommendation of previous researchers, we believed the interviews would provide further validation for our findings (Webb et al. 1966). Collecting different kinds of data on the same phenomenon improves the accuracy of researcher judgments (Jick 1979). Thirty-seven of the initial 48 subjects participated in this phase (i.e., 16 business executives and 21 security executives). The interviews were done via video conferencing and telephone sessions. They lasted an average of 40 minutes.

ANALYSIS AND RESULTS FOR Q1:

What are the factors that motivate subjects to participate in information security survey research?

The 1003 responses collected from phase one of the research were used to answer Q1. A content analysis of the responses identified seven main themes/categories and 33 individual items for them. Table 4 shows the results of the content analysis.

Table 4. Information Security Research Participation Factors

Survey Methodology and Design (SM) 1. Promise of anonymity 2. Convenience of completion (multiple methods) 3. Simplicity; a single, open-ended item 4. Upfront, initial information about the expectations 5. Nature of research did not require disclosure of intricate security details 6. Participation did not require disclosure of proprietary information 7. I could control the amount of time allocated 8. Assurance of confidentiality in terms of responses 9. Assurance that contact information would not be shared with other researchers 10. Request for participation was done face-to-face
Topic (TO) 11. Interesting and useful 12. Importance 13. Urgency 14. Relevance 15. Timely (need to get the most bang for buck in this economy) 16. Information collected did not present a risk to my company
Researcher characteristics/attributes (RC) 17. Persistence (multiple attempts to solicit participation) 18. Reputation and credentials 19. Trustworthiness and honesty – willing to sign disclosure 20. Persuasiveness 21. Personable and available 22. Conscious of and respectful of my time 23. Confident and knowledgeable about the subject matter
Knowledge Enhancement (KE) 24. Possibility of gaining knowledge to improve security at my firm 25. Improving knowledge about how to allocate scarce security resources 26. Gaining direct access to such info might help my org to be more competitive

Benchmarking (BM)
27. Curious about what others are doing
28. Access to knowledge about what peers are doing
Incentive (IN)
29. Assurance of receiving a report of the findings
30. Offer to personally discuss the findings with my firm employees
Subjective Norms (SN)(i.e., influence of people/entities in one's social environment)
31. Other organizations were willing to participate; I didn't want to miss out on the chance to have access to important information
32. My company encouraged participation
33. Sponsoring organization encouraged participation

ANALYSIS AND RESULTS FOR Q2:

Do business and security subjects' reasons for participation in information security survey research differ?

The data collected from the second phase of the research was used to answer question 2. Although descriptive analysis alone of the responses from phase one of the research could have been used to answer question 2, we chose to use the independent t-test because it would indicate not only the specific areas where business and security executives differed, but also provide some evidence about the significance of the differences. The business and security executives' reasons for participating in the research differed for 14 of the 33 items. For example, business executives were more likely to participate than security executives because upfront, initial information about the expectations of the research were offered (i.e., item SM4 in Table 4) and because the topic was important and relevant (items TO12 and TO14, respectively, in Table 4). However, the more significant reasons for security executives than business executives were subjective norm items such as the extent to which other respondents participated (SN31) and their own company's approval of participation (SN32). Table 5 shows the items as well as their means for the two subject types. The item column uses the abbreviations indicated in Table 4.

Table 5. Difference in Business and Security Executives' Participation Reasons

Item	Business Mean	Security Mean	t
SM1	5.00	4.95	1.00
SM2	5.00	4.91	1.00
SM3	4.77	4.73	.37
SM4	5.00	4.77	2.02*
SM5	5.00	5.00	N/A
SM6	5.00	4.86	1.37
SM7	4.55	4.23	1.37
SM8	5.00	4.95	1.00
SM9	3.45	4.18	1.16
SM10	4.86	4.64	.96
TO11	4.36	4.41	.27
TO12	4.95	3.00	9.18***
TO13	3.14	3.05	.42
TO14	4.59	3.27	6.92***
TO15	5.00	4.86	1.00
TO16	5.00	5.00	N/A
RC17	4.32	3.68	1.96*
RC18	4.77	4.50	2.81**
RC19	4.05	2.09	10.20***
RC20	5.00	4.50	3.92***
RC21	2.95	2.68	.71
RC22	4.00	4.14	.45
RC23	5.00	4.95	1.00
KE24	5.00	3.68	6.54***
KE25	4.96	3.64	8.63***
KE26	4.91	2.45	14.38***
BM27	4.59	3.09	13.75***
BM28	3.95	3.55	1.44
IN29	4.77	3.27	7.71***
IN30	4.27	3.82	1.74
SN31	2.18	3.23	2.88**
SN32	2.59	3.64	3.43***
SN33	4.55	4.68	.378

N/A – The two means are identical, thus there is no difference (i.e., t-value could not be computed).

*p < .05, **p < .01, *** p < .001.

The overall mean for the business and security executives was respectively, 4.43 and 4.01 ($t=3.81$, $p<.001$). Thus, there was an overall difference in their reasons for participating in the research.

ANALYSIS AND RESULTS FOR Q3:

Does industry type influence the reasons subjects agree to participate in information security survey research?

Correspondence analysis (CA), using SPSS version 20, was employed to answer Q3. CA is a perceptual mapping technique that shows visual relationships and differences among data. Its objective is to geometrically show data as a set of row and column points in a dimensional space (Yavas and Shemwell 1996). The Chi-square statistic indicates the difference between the rows and columns of data. Mathematically, it is similar to principal component analysis because it decomposes the Chi-square measure into components (Greenacre 1989). More specific for the current study, CA shows differences and similarities between the rows (i.e., the 13 industries) and the columns (i.e., survey participation factors, as shown in table 4).

Because the objective of correspondence analysis is to represent the data graphically to show the relationships between the variables of interest, it allows easier interpretation of the results. A perceptual map produced by CA is capable of providing "a better understanding and certainly more easily present relations from a picture than from a large table of coefficients", (SPSS 1998, p. 1-1). For example, CA has been used in information systems research to study strategic information systems planning (Remenyi 1992), website characteristics (Jowkar and Didegah 2010), and information retrieval systems (Bigot et al. 2011).

The 1003 responses collected from phase one of the research and the content analysis categories, as shown in table 4, were used to construct the frequency table for the correspondence analysis. Because some industries were represented by more than one organization, the average number of responses for each industry was used, as done in previous research (Ivy 2001). Eigenvalues and the cumulative variance explained by the dimensions were used to determine the dimensionality of the solution. Table 6 shows that one dimension will explain 55.2% of the total data variability and that two dimensions will explain more than 77% of the variability, which indicated that more than three-fourths of the variability could be explained by using two dimensions. Therefore, a two-dimensional solution was deemed sufficient for this study (Ivy 2001).

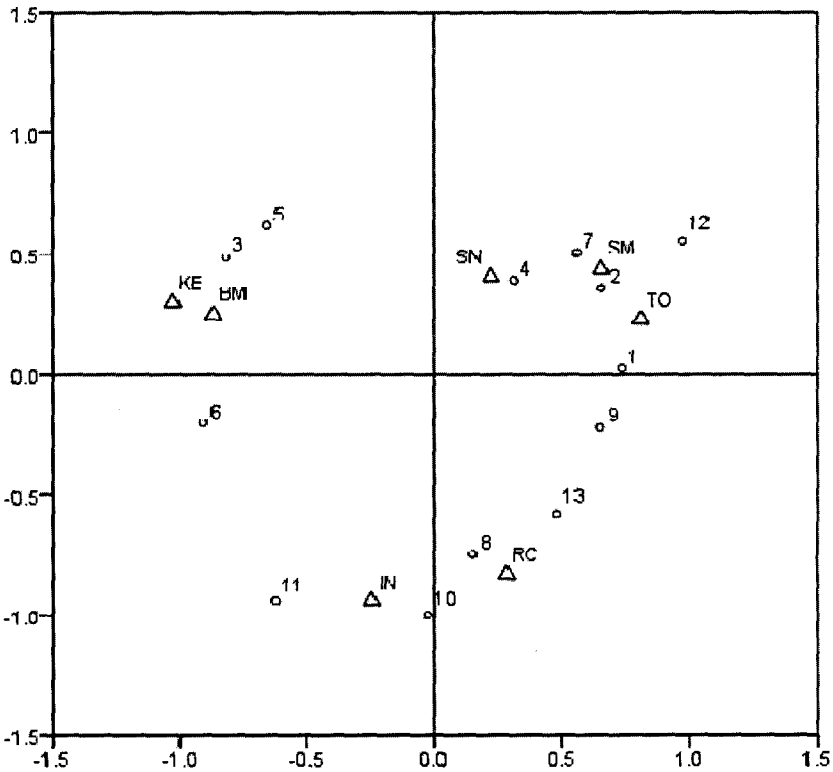
Table 6. Summary of Dimension Results

Dimension	Singular value	Inertia	Proportion of Inertia Accounted for	Cumulative	Std. Dev.	Correlation
1	.457	.209	.552	.552	.027	.127
2	.289	.084	.221	.773	.031	
3	.190	.036	.096	.869		
4	.162	.026	.069	.938		
5	.140	.020	.052	.990		
6	.061	.004	.010	1.000		
Total		.378	1.000	1.000		

($X^2 = 379.498$, $p<.001$)

Figure 1 shows a perceptual map of the seven survey participation factors and the 13 industries. Directly below the figure is the key which is needed to interpret the map. The finance, healthcare, and insurance industries were more closely aligned with the benchmarking and knowledge enhancement factors than other industries. In contrast, government industry participants were more concerned with subjective norms than any of the other participating industries. Participants in the entertainment and manufacturing industries closely identified with survey methodology and design attributes whereas publishing industry participants identified with researcher characteristics.

Figure 1. Perceptual Map Showing Relative Distances with Participation Factors



Map Key

SM = Survey Methodology and Design

TO – Topic

RC = Researcher characteristics/attributes

KE = Knowledge Enhancement

BM = Benchmarking

IN = Incentive

SN = Subjective Norms

1 = Education

2 = Entertainment

3 = Finance

4 = Government

5 = Healthcare

6= Insurance

7 = Manufacturing

8 = Publishing

9 = Real Estate

10 = Restaurant

11 = Retail

12 = Transportation

13 = Utilities

DISCUSSION OF FINDINGS

The content analysis of ISSR participation factors largely confirmed previous research that had emphasized the importance of survey methodology (Chesney 2006; Schleifer 1986), topic salience (Groves et al. 2004; Roose et al. 2007), researcher characteristics (Schleifer 1986; Singer and Kohnke-Aguirre 1979), and the presence of incentives (Groves et a. 1992; Halpern et al. 2004) as reasons for subject participation in research. However, three other factors emerged as a result of the current research. One was knowledge enhancement. Executives agreed to participate because they thought doing so might provide knowledge that would improve their own organization's information security, help to improve allocation of scarce security resources, and improve their firm's competitiveness. This finding was consistent with recent research that had identified knowledge as an important organizational asset with the capability to create competitive advantage as well as facilitate productivity and innovation (Teece 1998). Furthermore, Landry and Amara's (2012) knowledge transfer model proposed that organizations do "recognize the potential value of knowledge-based opportunities" (p. 95). Managers are able to transform that potential into actual value to ultimately improve their organizations.

An interesting finding about the results of the content analysis was that many of the factors that motivated participation in ISSR were not overtly related to information security or IT issues. This confirmed previous research that had suggested that information security is about more than technological issues (Slusky and Partow-Navid 2012).

A second emerging factor was benchmarking. Participants were curious about the processes used in other organizations. As one executive emphasized during an interview, "I want to know what the premier organizations are doing. Participating in your research was one way to find out." Similarly, another executive stated, "No one at other firms will discuss their security investments with you ... and I understand why. However, my participation grants me some access to that information." Although our *a priori* literature review about reasons why an individual might participate in research did not indicate benchmarking as a reason, it was not surprising that it emerged as a factor because it had been frequently identified as a way to achieve competitiveness (Camp 1989). Moreover, a 1995 study found that more than 60% of the firms across all sectors had engaged in benchmarking (Zairi and Sinclair 1995). Furthermore, researchers had often emphasized the need for firms to improve their performance by looking outside their companies to obtain best practices from other organizations (Camp 1989).

The third emerging factor, subjective norms, referred to the influence of people or entities in one's environment. Subjects were influenced by their perception that other organizations would participate, their own company's encouragement to participate, and the sponsoring firm's support for the research. This finding was consistent with the Theory of Reasoned Action (Ajzen and Fishbein 1980) which had predicted that

other individuals' approval of certain behavior positively affected the likelihood that one would engage in that same behavior. Also, assuming that the subjects had high regard for the research sponsor, it is reasonable to expect that sponsorship would result in an increased response rate (Groves et al. 2000)

In general the reasons that influenced business and security executives to participate in information security research differed (i.e., business executives' mean was 4.43 and security executives' mean was 4.01 with $p<.001$) thus confirming the stream of research about perceptual differences between business and technical managers (Rainer et al. 2007; Tai and Phelps 2000). However, the specific differences were interesting. Although there were statistical differences in business and security respondents' answers for 14 of the 33 reasons, the only reasons that were more influential for the security executives were in the subjective norms category. Perhaps, the difference in organizational hierarchy levels of the subjects (i.e., CEO level was higher than that of the security executive) influenced their reasons for participating. Similarly, perhaps their individual decision-making styles combined with their different experiences or knowledge bases contributed to their assessments of the participation factors.

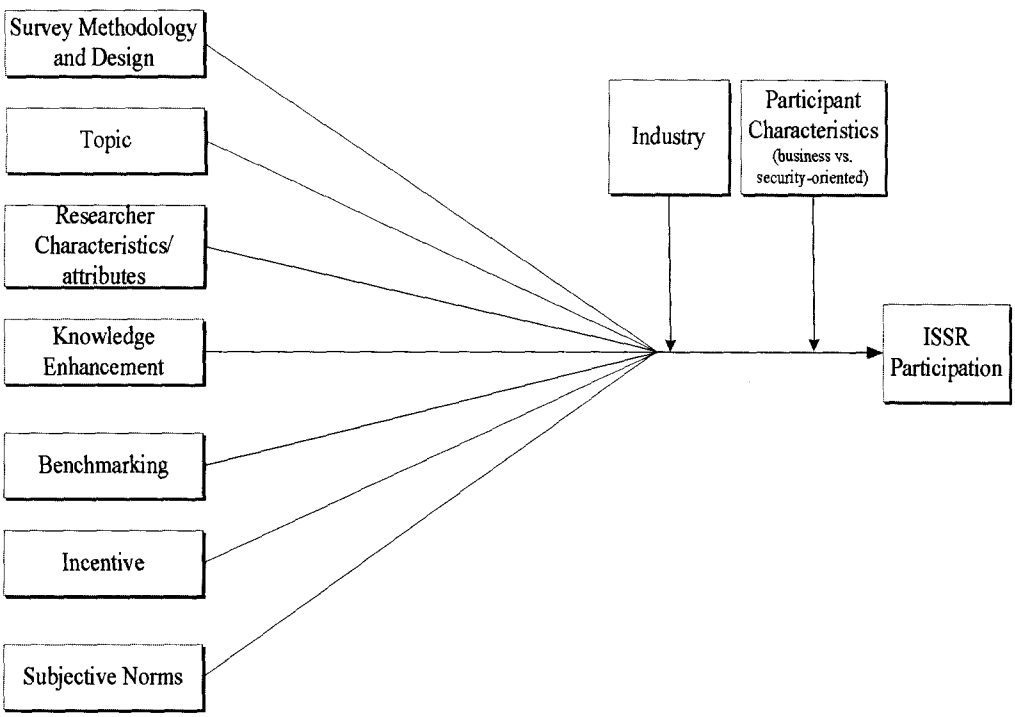
Finally, we found that a participant's decision to participate was affected by industry type. That finding was consistent with previous literature that had emphasized the importance of delineating industry characteristics when designing research (Mauri and Michaels 1998). However, an important contribution of the current research was the identification of characteristics that matched a specific industry type. Perhaps, the degree of information intensiveness in the industry influenced the results. Although the statistical analysis indicated industry differences, interviews conducted in phase 3 of the research corroborated this finding.

In addition to the open-ended question where subjects shared their reasons for participating in the research, each had also responded to the scaled item that rated the extent to which their participation had benefitted their organization. During the interviews, subjects were asked to provide more feedback particularly about their reasons for participating and how (if any) their organization had benefitted by engaging in the survey. Participants in the finance, healthcare, and insurance industries were more eager to discuss the competitive benefits of participating. For example, one such participant in the finance industry said, "I viewed this as a great opportunity to know what my competitors might be doing. If they're investing in some security that we are not investing in, then I want to know about it .... and I want to know why we aren't at least considering it." Likewise, another in the healthcare industry stated, "We cannot survive unless we are conscious about information security. If we don't take notice of what is available in that area, we will not continue to thrive. Participating in this research helped me to improve my knowledge about allocating funds for information security. I might now consider putting some dollars in places where I have not done so in the past." Participants in these three industries were clearly more strategic about their reasons for participating in the research and thus their perceived benefits of doing so.

In contrast, the government industry participants emphasized benefits quite differently than those in finance, healthcare, and insurance. In general they expressed an interest in being a "team player" in regard to their relationship with peer organizations and to positively responding to the sponsor's request to participate in the research. One government industry executive stated, "I didn't see the harm in participating and it also helps to establish and maintain goodwill with your sponsor." Another said, "Your research was attracting participation from some well-respected companies, so I decided to participate too. Maybe my organization can learn something from them."

Unquestionably, organizations' reasons for participating in ISSR, as well as their perceptions of the value of doing so, are mixed. However, based on the findings from the current study, we offer the following model of information security survey research participation, as shown in figure 2. It shows seven independent variables that might influence ISSR participation and the dependent variable which is ISSR participation. Industry and participant characteristics (i.e., business vs. security-oriented) are shown as moderating variables.

Figure 2. Model of Information Security Survey Research Participation



IMPLICATIONS

The research identified a number of factors that influenced participation in ISSR as well as a framework that might be used to inspire future such research. Studies could be conducted to reduce the factors to a more parsimonious set of dimensions and items. Perhaps, researchers could determine which factors are greater triggers for obtaining participation in ISSR. Knowing such information would help to identify a smaller set of factors for future research. Likewise, researchers might want to provide further validation for the proposed model of information security survey research participation with a larger sample size.

An interesting contribution of the study was the identification of knowledge enhancement, benchmarking, and subjective norms as factors that motivated participation in ISSR. Researchers might want to emphasize these features when making their appeals for participation. For example, subjects in the current study clearly viewed their participation as an opportunity to engage in benchmarking activities and gather knowledge to benefit their organizations. Therefore, researchers could specifically identify the types of knowledge that might be obtained by participating in a survey and how that knowledge might benefit an organization. Similarly, practitioners might need training to help them understand how to view their participation in surveys as benchmarking and knowledge-based opportunities.
The emergence of subjective norms as a participation factor provided some evidence that more emphasis is needed to stress to potential subjects the social benefits of participating in information security surveys. Because encouragement from the subject's firm motivated participation, perhaps researchers should consider gaining the initial support of top executives for their research prior to approaching the end recipient of the survey. This method has been practiced in previous information systems research (e.g., Sabherwahl and Chan 2001). Also, the presence of a sponsor motivated participation in the current study. Sponsorship included active solicitation and encouragement of the executives to participate in the survey. Although sponsored research is sometimes difficult to obtain, we recommend that information security survey researchers identify more opportunities to engage in such work to perhaps increase response rates.

The reasons that influenced business and security executives to participate in information security surveys differed. Although we speculated that the difference in organizational hierarchy levels, decision-making styles, and knowledge bases might have influenced the results, additional research is needed to test that speculation or identify other reasons for the differences.

The study found that industry type influenced the decision to participate. We identified characteristics that matched specific industries and speculated that variations in industry information intensiveness might have been responsible for the observed differences in the decision to participate in the survey. Further research is needed to test this theory.
The term "research" is a broad term. However, survey research is limited to the process of assessing one's thoughts, opinion, or feelings (Shaughnessy et al. 2011).

The current study investigated motivations for participating in information security survey research. Future research could determine if these results generalize to other types of information security research. Similarly, the current research was limited to business and security executives as the participants. Future research must examine the generalizability of these results to other security and business professionals.

CONCLUSION

Considering the pervasive use of IT in organizations, information security has become increasingly important. However, research about information security is necessary in order to recognize improvements in that area. Such research often requires the cooperation of willing participants.

Obtaining subject participation in research in general is undoubtedly challenging. However, because of the sensitive nature of information security activities, potential respondents for such research are more hesitant about participation. This study has identified potential factors that might improve response rates for future information security survey research. It suggests that researchers might want to be more attentive to the industry selected and thus highlight characteristics of interest for that particular industry when soliciting participation. Similarly, tailoring might be needed to appeal to individual subject attributes because the current study showed that business and security executives' reasons for participating in research are different. Future research could test these findings on a larger sample and also identify other factors that influence participation in information security survey research.

REFERENCES

Abraham, S. 2011. "Information Security Behavior: Factors and Research Directions," in *Proceedings of the Seventeenth Americas Conference on Information Systems*, August 4-7, Michigan: AIS, pp. 1-13.

Ajzen, I., and Fishbein, M. 1980. *Understanding Attitudes and Predicting Social Behavior*. Englewood Cliff, NJ: Prentice Hall.

Allan, G. 2003. "A Critique of Using Grounded Theory as a Research Method," Electronic *Journal of Business Research Methods* (2:1), pp. 1-10.

Bigot, A., Chrisment, C., Dkaki, T., Hubert, G., and Mothe, J. 2011. "Fusing Different Information Retrieval Systems According to Query-topics: A Study Based on Correlation in Information Retrieval Systems and TREC Topics," *Information Retrieval* (14), pp. 617-648.

Camp, R.C. 1989. *Benchmarking: The Search for Industry Best Practices that Lead to Superior Performance*. Milwaukee, WI: ASQC Quality Press.

Chesney, T. 2006. "The Effect of Communication Medium on Research Participation Decisions," *Journal of Computer-mediated Communication* (11), pp. 877-883.

Cohen, J. A. 1960. "A Coefficient of Agreement for Nominal Scales," Educational and Psychological Measurement (20), pp. 37-46.

CSI (2010/2011).*Computer Crime and Security Survey*. Computer Security Institute Website: (http://www.gocsi.com; accessed April 4, 2013).

Csrc.nist.gov. 2002. *Federal Information Security Management Act of 2002 (Title III of E-Gov)*.National Institute of Standards and Technology Website (http://csrc.nist.gov/drivers/documents/FISMA-final.pdf; accessed August 1, 2013).

Denning, P. J. 1992. "Passwords," *American Scientist* (80), pp. 117-120.

Diaz, P., Aedo, A., and Ribagorda, A. 1998. "A Security Model for the Design of Hypermedia Systems," in *Proceedings of the TC11 14th International Conference on Information Security*, pp. 251-260.

Dillman, D. A. 2000. *Mail and Internet Surveys: The Tailored Design Method, 2nd edition*. New York, NY: Wiley.

Galea, S. and Tracy, M.2007. "Participation Rates in Epidemiologic Studies," *AEP*(17:9), pp. 643-653.

Greenacre, M. J. 1989. "The Geometric Interpretation of Correspondence Approach," *Journal of the American Statistical Association* (82), pp. 437-447.

Groves, R. M., Presser, S., and Dipko, S. 2004. "The Role of Topic Interest in Survey Participation Decisions," *Public Opinion Quarterly*(68:1), pp. 2-31.

Groves, R. M., Cialdini, R. B., and Couper, M. P. 1992. "Understanding the Decision to Participate in a Survey," *Public Opinion Quarterly*(56:4), pp. 475-495.

Groves, R. and Couper, M. 1998.*Nonresponse in Household Interview Surveys*. New York: John Wiley and Sons.

Groves, R. M., Singer, E., and Corning, A. 2000. "Leverage-Saliency Theory of Survey Participation," *Public Opinion Quarterly*(64), pp. 299-308.

Halpern, S. D., Karlawish, J. H. T., Casarett, D., Berlin, J. A., and Asch, D. A. 2004."Empirical Assessment of Whether Moderate Payments are Undue or Unjust Inducements for Participation in Clinical Trials," *Archives of Internal Medicine* (164), pp. 801-803.

Hrebiniak, L. G. and Snow, C. C. 1980."Research Notes: Industry Differences in Environmental Uncertainty and Organizational Characteristics Related to Uncertainty," *Academy of Management Journal*(23:4), pp.750-759.

Ivy, J. 2001. "Higher Education Institution Image: A Correspondence Analysis Approach," *The International Journal of Educational Management* (15:6/7), pp. 276-282.

Jick, T. D. 1979. "Mixing Qualitative and Quantitative Methods: Triangulation in Action," *Administrative Science Quarterly* (24:4), pp. 602-611.

Johnson, A. M. 2009. "Business and Security Executives Views of Information Security Investment Drivers: Results From a Delphi Study," *Journal of Information Privacy & Security* (5:1), pp. 3-27.

Jowkar A. and Didegah, F. 2010. "Evaluating Iranian Newspapers' Web Sites Using Correspondence Analysis," *Library Hi Tech*, (28:1), pp. 119-130.

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

Krippendorff, K. 1980. *Content Analysis: An Introduction to Its Methodology*. Beverly Hills, CA: Sage Publications.

Lambrinoudakis, C. 2000. "Smart Card Technology for Deploying a Secure Information Management Framework," *Information Management & Computer Security* (8:4), pp. 173-183.

Landry, R. and Amara, N. 2012. "Elucidation and Enhancement of Knowledge and Technology Transfer Business Models," *VINE: The Journal of Information and Knowledge Management Systems* (42:1), pp. 94-116.

Leach, J. 2003. "Improving User Security Behavior," *Computers & Security* (22:8), pp. 685-692.

Luftman, J., and Derksen, B. 2012. "Key Issues for IT Executives 2012: Doing More with Less," *MIS Quarterly Executive*(11:4), pp. 207-218.

Ma, Q, and Pearson, J. M. 2005. "ISO 17799: 'Best Practices' in Information Security Management," *Communications of the Association for Information Systems* (15), pp. 577-591.

Mauri, A. J. and Michaels, M. P. 1998. "Firm and Industry Effects Within Strategic Management: An Empirical Examination," *Strategic Management Journal* (19), pp. 211-219.

Maynard, D. W., Freese, J., and Schaeffer, N. C. 2010. "Calling for Participation, Requests, Blocking Moves, and Rational (Inter)action in Survey Introductions," *American Sociological Review* (75:5), pp. 791-814.

Mayring, P. 2000. "Qualitative Content Analysis," *Forum: Qualitative Social Research* 1(2), article 20, (http://www.qualitative-research.net/index.php/fqs/article/view/1089/2386: accessed July 31, 2013).

Moore, G. C., and Benbasat, I. 1991. "Development of An Instrument to Measure the Perceptions of Adopting an Information Technology Innovation," *Information Systems Research* (2:3), pp. 192-222.

National Research Council.1979. *Privacy and Confidentiality as Factors in Survey Response.* Washington, DC: National Academy Press.

Oksenberg, L., Coleman, L, and Cannell, C. F. 1986."Interviewers' Voices and Refusal Rates in Telephone Surveys," *Public Opinion Quarterly*(50:1), pp. 97-111.

Preloran, M. H., Browner, C. H., and Lieber, E. (2001). "Strategies for Motivating Latino Couples' Participation in Qualitative Health Research and Their Effects on Sample Construction," *American Journal of Public Health*(91:11), pp. 1832-1841.

Rainer, R. J., Marshall, T. E., Knapp, K. J., and Montgomery, G. H. 2007. "Do Information Security Professionals and Business Managers View Information Security Issues Differently?" *Information Systems Security* (16:2), pp. 100-108.

Remenyi, D. 1992. "Researching Information Systems: Data Analysis Methodology Using Content and Correspondence Analysis," *Journal of Information Technology* (7), pp. 76-86.

Roose, H., Lievens, J., and Waege, H.2007. "The Joint Effect of Topic Interest and Follow-up Procedures on the Response in a Mail Questionnaire," *Sociological Methods & Research* (35:3), pp. 410-428.

Sabherwal, R. and Chan, Y. E. 2001. "Alignment Between Business and IS Strategies: A Study of Prospectors, Analyzers, and Defenders," *Information Systems Research* (12:1), pp. 11-33.

Saint-Germain, R. 2005. "Information Security Management Best Practice Based on ISO/IEC 17799," *The Information Management Journal*(July/August), pp. 60-66.

Sanginga, P. C., Tumwine, J., and Lilja, N. K. 2006. "Patterns of Participation in Farmers' Research Groups: Lessons From the Highlands of Southwestern Uganda," *Agriculture and Human Values* (23), pp. 501-512.

Schleifer, S. 1986. "Trends in Attitudes Towards and Participation in Survey Research," *Public Opinion Quarterly* (50), pp. 17-26.

Shaughnessy, J., Zechmeister, E., and Jeanne, Z. 2011. *Research Methods in Psychology, 9th edition*. New York, NY: McGraw Hill.

Singer, E., and Kohnke-Aguirre, L. (1979). "Interviewer Expectation Effects: A Replication and Extension," *Public Opinion Quarterly* (43:2), pp. 245-260.

Siponen, M. T. and Oinas-Kukkonen, H. 2007. "A Review of Information Security Issues and Respective Research Contributions," *Database for Advances in Information Systems* (38:1), pp. 60-80.

Slusky, L., and Partow-Navid, P. 2012. "Students Information Security Practices and Awareness," *Journal of Information Privacy & Security* (8:4), pp. 3-26.

Spears, J. L., and Barki, H. 2010. "User Participation in Information Systems Security Risk Management," *MIS Quarterly* (34:3), pp. 503-522.

SPSS 1998.*Perceptual Mapping Using SPSS Categories*. Chicago, IL: SPSS.

Steeh, C.1981. "Trends in Nonresponse Rates," *Public Opinion Quarterly*(45), pp. 40-57.

Tai, L A, and Phelps, R. 2000. "CEO and CIO Perceptions of Information Systems Strategy: Evidence from Hong Kong," *European Journal of Information Systems*(9:3), pp. 163-172.

Teece, D.J. 1998. "Capturing Value from Knowledge Assets: The New Economy, Markets for Know-how, and Intangible Assets," *California Management Review* (40), pp. 55-79.

Venkatraman, S., and Delpachitra, I. 2008. "Biometrics in Banking Security: A Case Study," *Information Management & Computer Security* (16:4), pp. 415-430.

Webb, E.J., Campbell, D. T., Schwartz, R. D. and Sechrest, L. 1966. *Unobtrusive Measures: Non-reactive Research In the Social Sciences*. Chicago: Rand McNally.

Yavas, U. and Shemwell, D. J.1996. "Bank Image: Exposition and Illustration of Correspondence Analysis," *International Journal of Bank Marketing*(14:1), pp. 15-21.

Zairi, M, and Sinclair, D. 1995. "Business Process Reengineering and Process Management: A Survey of Current Practice and Future Trends in Integrated Management," *Management Decision* (33:3), pp. 3-16.

Zhang, L. and Amos, C. 2012. "A Model of End Users' Web Threats Information Processing," *Journal of Information Privacy & Security* (8:3), pp. 15-36.

AUTHOR BIOGRAPHY

Dr. Alice M. Johnson is an associate professor in the School of Business and Economics at North Carolina Agricultural and Technical State University. She holds a B.A. in Business Administration from Winston-Salem State University, an M.S. in Personnel and Industrial Relations from Winthrop University, and a Ph.D. in Decision Sciences and Information Systems from the Gatton College of Business and Economics at the University of Kentucky. She is a Certified Information Systems Auditor (CISA). Her research has previously appeared in the *Journal of Management Information Systems*, *Information & Management*, the *Journal of Information Privacy and Security*, and elsewhere.

Dr. Belinda P. Shipps is an assistant professor in the School of Business and Economics at North Carolina Agricultural and Technical State University. She holds a B.A. in Education from Michigan State University, an M.S. in Management Information Systems from the University of Wisconsin-Milwaukee, and a Ph.D. in Management Information Systems from the Lubar School of Business at the University of Wisconsin-Milwaukee. Her research interests include: IT security, sourcing/staffing issues and strategies, social networking and education.

APPENDIX: INSTRUCTIONS TO RESPONDENTS AND THE SURVEY PHASES

The business and security executives responded to all items. Variable names (such as SMn) did not appear in the original instrument and the items did not appear in the exact order indicate here. However, this was done here for clarification.

Phase One (Open-ended Reasons for Participation)

You recently participated in a study about information security investment and have agreed to share your reasons for doing so. (Thanks !!!)

Please use the space below to indicate the reasons you decided to participate (one box per reason). If at all possible, please list at least ten (10) reasons. If more space is required to list your reasons, please continue on the back of this page which contains additional numbered boxes. If additional space is needed after using the back of this sheet, feel free to add pages to provide complete feedback about your reasons for participating in the study. Upon completion, please use the pre-paid envelope to return your feedback.

If we have questions about your feedback, may we contact you for clarification? Yes____ No____

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.

Phase Two (Scaled Items – Reasons for Participation)

Please indicate on a scale of 1 (no extent) to 5 (great extent) the extent to which the indicated reason motivated you to participate in the information security investment study.

	Reason	No Extent				Great Extent
SM1:	Promise of anonymity	1	2	3	4	5
SM2:	Convenience of completing the survey	1	2	3	4	5
SM3:	Simplicity; a single open-ended question	1	2	3	4	5
SM4:	Upfront, initial information about the expectation were provided	1	2	3	4	5
SM5:	Nature of the research did not require disclosure of intricate security details	1	2	3	4	5
SM6:	Participation did not require disclosure of proprietary information	1	2	3	4	5
SM7:	I could control the amount of time allocated	1	2	3	4	5
SM8:	I was assured my responses would be confidential	1	2	3	4	5
SM9:	I was assured my contact information would not be shared with other researchers	1	2	3	4	5
SM10:	Initial request for participation was done face-to-face	1	2	3	4	5
TO11:	Topic was interesting and useful	1	2	3	4	5
TO12:	Topic was important	1	2	3	4	5
TO13:	Topic was urgent	1	2	3	4	5
TO14:	Topic was relevant	1	2	3	4	5
TO15:	Topic was timely and would help me get the most bang for my buck in this economy	1	2	3	4	5
TO16:	Information collected did not present a risk to my company	1	2	3	4	5
RC17:	The researcher was persistent	1	2	3	4	5
RC18:	The researcher reputation and credentials were impressive	1	2	3	4	5
RC19:	The researcher appeared to be trustworthy and honest	1	2	3	4	5
RC20:	The researcher was persuasive	1	2	3	4	5
RC21:	The researcher was personable and available for questions	1	2	3	4	5
RC22:	The researcher was conscious of and respectful of my time	1	2	3	4	5
RC23:	The researcher was confident and knowledgeable about the subject matter	1	2	3	4	5
KE24:	I could possibly gain knowledge to improve security at my firm	1	2	3	4	5
KE25:	I might gain knowledge about how to allocate scarce security resources	1	2	3	4	5
KE26:	I might gain knowledge to help my organization be more competitive	1	2	3	4	5
BM27:	I was curious about what other companies are doing	1	2	3	4	5
BM28:	I wanted access to knowledge about what my peer firms are doing	1	2	3	4	5
IN29:	I was assured that I would receive a report of the findings	1	2	3	4	5
IN30:	The researcher offered to personally discuss the findings with my employees	1	2	3	4	5
SN31:	Other organizations were willing to participate	1	2	3	4	5
SN32:	My company encouraged participation	1	2	3	4	5
SN33:	The research sponsor encouraged participation	1	2	3	4	5
	Indicate on a scale of 1 to 5, the extent to which your participation in the survey has benefitted your organization.	1	2	3	4	5

Phase Three (Interviews)

A copy of each subject's responses received for phase one of the survey was sent to the participant prior to the interview. The interviews were governed by the three leading open-ended items shown below. Then, based on the responses, other questions were asked and answered.

1. Please briefly review your list of (x) reasons that motivated you to participate in the information security investment study. Let's discuss the two reasons you feel motivated you more than the others.

2. Please feel free to elaborate about any of the other reasons that motivated your participation.

3. How has your participation benefited you or your organization?