Information Security and Task Interdependence: An Exploratory Investigation

Kenneth J. Knapp
Department of Management
U.S. Air Force Academy, Colorado
Email: kenneth.knapp@usafa.edu

Thomas E. Marshall
College of Business
Auburn University, Alabama
Email: marshall@business.auburn.edu

Abstract

This sequential qualitative-quantitative study investigates reported levels of task interdependence by certified information security professionals from organizations worldwide. The empirical tests show that information security ranked high in task interdependence compared to other information system related tasks. Additionally, comparing results from a different survey, information security work demonstrates higher levels of reported task interdependence than telecommunications software development work. We present the results of a demographic analysis of the survey taken by 936 certified information security professionals. Overall, the results suggest that information security work in organizations requires high levels of task interdependence. These findings have implications for researchers by identifying task interdependence-related topics for future study. For practitioners, these findings provide relevant insight into the nature of information security work in organizations.

1. Introduction

With national economies fully dependent upon information technology for survival [1], information security has become a paramount issue facing organizations worldwide. Yet, one can find evidence of a deplorable state of information security in the frequency of media reports about security breaches [e.g. 2], system vulnerabilities [e.g. 3] and from published survey data [e.g., 4, 5]. One analysis found that security incidents can cost companies between $17 and $28 million for each occurrence [6]. Because information security incidents are frequent and costly, management must take security seriously to protect organizational information.

Noting the disappointing state of information security in organizations, Dhillon & Backhouse [7] called for more empirical research to develop key principles that will help in the management of information security. Despite the call, few published organizational studies report empirical investigations into information security issues [8]. This paper helps to fill the gap by investigating the role of task interdependence in organizational information security work. Researchers define task interdependence as the level to which employees rely upon other employees and resources to carry out a job. To our knowledge, no published research has extended the topic of task interdependence to the important domain of information security. Investigating the degree to which this area requires task interdependence can help researchers and practitioners alike understand more about the nature and demands of information security work.

Definitions vary on what information security work entails. Broadly defined, security represents the quality or state of being secure and free from dangers. To be secure is to receive protection from adversaries and other hazards [9]. The importance of information security often becomes critical in threatening and hostile environments. Security can be broken down into six basic functions: avoidance, deterrence, prevention, detection, recovery, and correction [10] with an overall goal of reducing risk to acceptable levels. Information security is a more recent phenomenon corresponding to the rise of computers, networks and the global Internet. A national U.S. standard acknowledges a shared responsibility by stating, "information security is multidisciplinary in nature, requiring a wide spectrum of knowledge such as operations security, emanations security, physical security, personnel security and related security areas" [11, p. 4]. A recognized international standard defines information security as

Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07)
0-7695-2755-8/07 $20.00 © 2007 IEEE

the preservation of confidentiality, integrity and availability of information. The standard encourages "a multi-disciplinary approach to information security that involves co-operation and collaboration of managers, users, administrators, application designers, auditors, and security staff, and specialists skills such as insurance and risk management" [12, p. 2]. The standard suggests that information security workers need to cooperate with others in an organization in order to preserve and protect information. Yet, the priority of information security can vary depending on an organization's external environment. For example, organizations in information-intensive sectors such as finance, banking, healthcare, and other heavily regulated sectors may place a higher priority on information security than organizations in other sectors. Overall, based on these definitions, information security cannot be limited to the computer technologists alone and requires a degree of organizational cooperation if security goals are to be accomplished.

The next section describes how the research question of this study came about through a qualitative analysis of responses to open-ended questions. We then review the task interdependence literature and identify two scales appropriate for this project. We provide quantitative results from giving these scales to samples of information security professionals and include a comparison of results to those in published studies. We then present a demographic analysis of our survey data. This paper concludes with implications for research and practice while suggesting topics for future study.

2. Preliminary Analysis

Data collection began with a posted announcement on the International Information Systems Security Certification Consortium [(ISC)^2] web site (www.isc2.org) calling for Certified Information System Security Professionals (CISSPs) to volunteer in a related research endeavor. (ISC)^2 is a non-profit, ISO/IEC 17024[1] compliant organization that manages the CISSP program. Among the requirements to earn a CISSP designation, candidates must pass a rigorous exam, consent to an ethical code of behavior, and possess a minimum of four years of professional experience in the field or three years experience plus a college degree. Maintaining certification requires a CISSP to earn continuing professional education credits.

In all, 348 CISSPs responded to the announcement and we sent them the following initial open-ended question via email: What are the top five information security issues facing organizations today? To this question, 220 participants provided usable responses giving a short title and rationale for each of their five issues. In the process of gathering and analyzing the responses, we asked several follow-on questions both to the entire sample (N=220) and to specific individuals for the purpose of obtaining clarifications, getting additional details, or receiving feedback on researcher analysis. In the end, we accumulated a database containing over 146,000 words of question responses suitable for the purposes of our study.

Using content analysis, we coded respondent statements into logical categories where each category represented a critical information security issue until a list of over 50 logical categories emerged. At the beginning of this project, we did not intend to investigate the concept of task interdependence. It was only after we discovered this meta-theme in the qualitative data that we began a literature review, ultimately focusing on the concept. While the study participants did not explicitly identify the issue of task interdependence in their responses, many discussed this notion while identifying other critical issues. After analyzing the responses, it became clear that task cooperation and coordination was an important meta-theme cutting across the categories found in the data. Table 1 provides typical respondent statements that illustrate this finding.

Table 1. Statements on security cooperation

"Official Information Security policy establishment and enforcement requires cooperation and coordination of IT Management, Human Resources, Legal, and Executive Management."
"Security is dependent upon cooperation of people. If people are not sold on the need, they will sabotage all good intentions."
"In order for our INFOSEC policy to be effective, it is necessary for all our units to cooperate, implement, and enforce the policy."
"The lack of cooperation between different internal functions, whether it is legal, (the) security team, audit and development, etc, causes a rupture in the security process. I have experienced a situation where different, competing security functions within the same organization do not share information or collaborate. This causes ends up causing problems

[1] The International Standards Organization/The International Electrotechnical Commission, (ISO/IEC) 17024 provides general requirements for bodies operating certification of persons. See www.iso.org.

in the long run, is inefficient, and is even dangerous."
"Devices like a Firewall are often actually managed and configured by Network Engineers, while the rules are designed by Security Engineers….When a single device requires the cooperation of what are all too often, opposing organizations, problems can occur."

3. Literature Search

The substantial number of qualitative comments about the importance of cooperation in information security led us to search the literature for appropriate constructs that would accurately capture the phenomena found in the responses. The concept of task interdependence accurately conveyed our finding. Task interdependence is defined as the extent to which individuals depend upon other individuals and resources to perform a job [13]. In the organizational literature, we found a considerable amount of research into this topic. Thompson [14] identified organizational routines involving considerable levels of material, resource, and information exchange to be environments high in task interdependence. Task interdependence underpins workflow patterns and routines that involve multiple actors whose habituated patterns of interdependent actions produce and reproduce an institutional context [15, 16]. Highly interdependent teams can lack incentives to cooperate if goal interdependence is relatively low [13, 17]. Establishing common group goals is one way to improve cooperation and productivity on highly interdependent information technology tasks [18]. One study found that high levels of task interdependence has been linked to high demands for top management support in order to improve the likelihood of information system implementation success [15]. Thus, top management can play an important role in establishing goals in environments high in task interdependence.

In the information systems (IS) literature, with notable exceptions [e.g. 15, 16, 18], the topic of task interdependence has received modest research attention with most of the research published outside of the IS domain. Our review did not find a published study directly investigating how information security work exhibits task interdependence. Yet, the concept that information security entails higher levels of task interdependence has support in the literature. In one analysis, new information security threats necessitate an increased level of computer literacy of the workforce and an interdependence between information security and organizational business processes [19]. In another analysis, a recognized information security practitioner believes that information security has changed over the years to the point that is it now a multi-disciplinary and multi-departmental function requiring a team-based approach for success [20].

Our study builds upon the idea that security requires a cooperative, team-based approach by investigating the measure of task interdependence in information security work using two previously developed scales [13, 21] and comparing the results to those in published studies [13, 15]. By doing so, we aim to provide insight into the interdependent nature of information security work. We did not find a comparable research project in the existing literature. To this end, based on our analysis of the qualitative data and of the literature, we offer the following proposition:

Information security work in organizations exhibits high levels of task interdependence.

In the next section, we present the quantitative results from investigating this proposition.

4. Quantitative Results

We investigate the proposition using two different surveys. First, we use the Pearce et al [21] scale with a small sample (N=68) to measure task interdependence in information security. Second, after the initial results indicated high levels of task interdependence, we use the Van der Vegt et al [13] scale to further investigate the proposition with a larger sample (N=936). Then, we offer a demographic analysis of the second survey's results.

4.1. Pearce et al Scale

Sharma & Yetton [15] conducted a meta-analysis of 22 studies that operationalized the *management support* and *information systems implementation success* variables. In their meta-analysis, three raters independently evaluated 22 information system tasks from published studies using the task interdependence scale from Pearce et al [21]. Our study used the same scale with a convenience sample of 68 CISSPs. The items use a five-point Likert scale (1=strongly disagree, 5=strongly agree). Table 2 provides the results. The internal validity was acceptable ($\alpha = 0.87$) and the scale sum was a 22.9. In Table 3, we reproduced the top 9 of 22 studies in Sharma & Yetton's meta-analysis results while inserting the results of the present study. As illustrated in the table, information security ranked third compared to the twenty-two IS tasks from the meta-analysis. While recognizing the limitations of this comparison based on the different methods used

between the two studies, this finding nevertheless provided preliminary evidence in favor of the proposition and justified further exploration of the topic.

Table 2. Pearce et al scale results (N=68)

Item	Mean	S.D.
1) Security-related tasks can be performed fairly independently of others. (Reverse Code)	2.37	0.96
2) Security-related tasks can be planned with little need to coordinate with others. (RC)	2.03	0.90
3) It is rarely required to obtain information from others to complete security-related tasks. (RC)	2.07	1.11
4) Information security-related tasks are relatively unaffected by the performance of others individuals or departments. (RC)	2.37	1.02
5) Information security-related tasks require frequent coordination with the effort of others.	3.84	0.89
6) Performance on information security-related tasks is dependent on receiving accurate information from others.	3.91	0.86

Table 3. Comparing other studies [15, p. 554]

Information System Application	Task Interdep.
Info Engineering using CASE tools	26.3
CASE tools	24.7
Information Security *(inserted)*	22.9
DSS Applications	21.2
DSS - Financial analysis & planning (3 studies)	20.7
OR/MS Projects	20.0
Sales forecasting model	19.7
Executive information systems	19.6
Telework	17.2
MLS Realty	14.4
Eleven other studies	7.7 - 13.7

4.2. Van der Vegt et al Scale (N=936)

A second task interdependence scale [13] was taken by 936 CISSPs who responded to a web posting by $(ISC)^2$ that was part of a related research study. The seven items with resulting mean and standard deviation are provided in Table 4. The first five items use a 5-point Likert scale (1=strongly disagree, 5=strongly agree). Item 6 has a range of 0-100 while item 7 has a range of 0-10. The questions refer to typical information security tasks performed in organizations.

Table 4. Task Interdependence Scale Results (N=936)

Item	Mean	S.D.
1) I have a one-person job; I rarely have to check or work with others. (RC).	1.9	.98
2) I have to work closely with my colleagues to do my work properly.	4.1	0.85
3) In order to complete our work, my colleagues and I have to exchange information and advice.	4.2	0.73
4) I depend on my colleagues for the completion of my work.	3.6	1.03
5) In order to complete their work, my colleagues have to obtain information and advice from me.	3.9	0.86
6) Indicate the percentage of your tasks for which you have to exchange information or cooperate with others in your organization.	62.4	24.87
7) Indicate the total number of hours per day you have to exchange information or cooperate with others to do your job well.	4.1	2.25

Because the responses to the items are on different scales, all seven items are standardized before combined into a single measure. The internal reliability was acceptable for both the five Likert-type items ($\alpha = 0.75$) and the seven combined items ($\alpha = 0.79$). Table 5 presents the Van der Vegt et al results involving a telecommunications group in the Netherlands and compares it to the present study results. The comparison suggests that information security exhibits higher level of task interdependence than telecommunications software work.

Table 5. Study Results Comparison

	Van der Vegt et al [13, p.719]	Present Study
Task	Telecommunications	Information Systems Security
Sample	129 members of 20 multidisciplinary teams from company in Netherlands; 70% of the teams work in software development	936 certified information systems security professionals (CISSPs) located worldwide in various industries.
Item 6	Mean = 32.10; S.D. = 28.8	Mean = 62.43; S.D.= 24.9
Item 7	Mean = 2.27; S.D. = 2.59	Mean = 4.11; S.D.= 2.25

4.3. Demographic Analysis

The large sample of 936 respondents allowed for a meaningful demographic analysis. The survey results vary across the sample including those demographics based on geographic location, sector, and organizational size. Figure 1 provides demographic results from fourteen categories describing internal organizational characteristics whereas Figure 2 provides fourteen categories of environmental factors. The figures illustrate the mean of the standardized items as well as the 95% confidence interval of the mean.

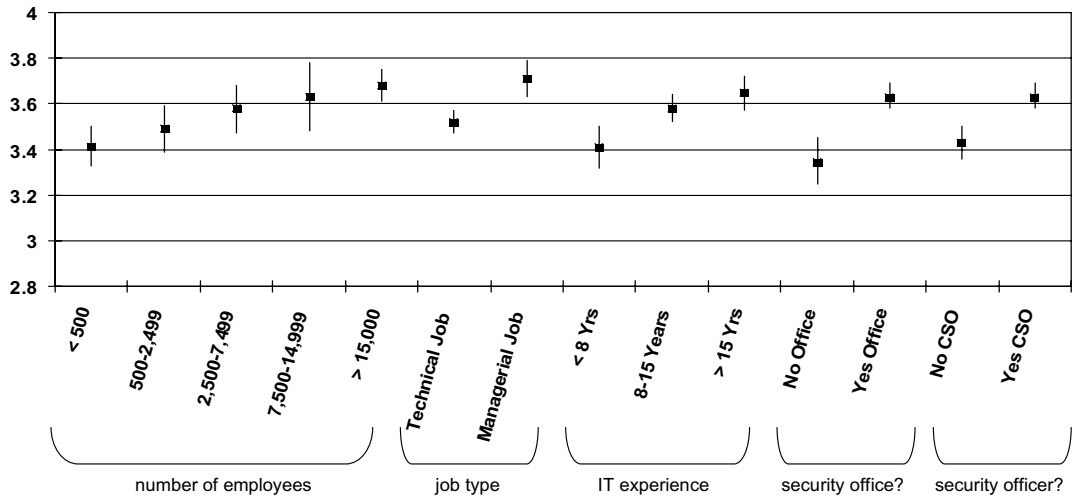

Figure 1. Task interdependence scores on organizational characteristics

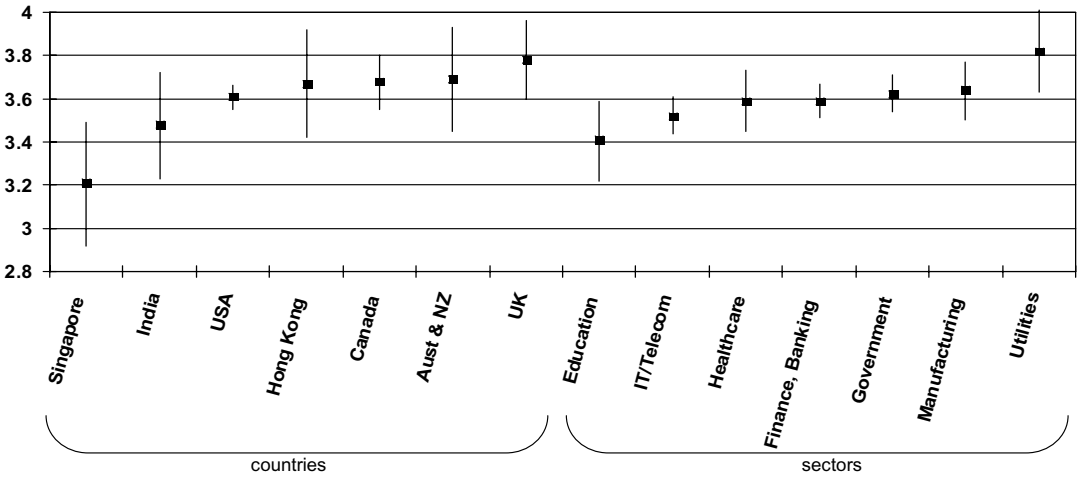

Figure 2. Task interdependence scores on environmental factors

An examination of Figure 1 reveals some significant and notable differences among the demographic sub samples. Here, we highlight four. First, organizational size had a significant effect on the results. The larger the organization, the higher the level of reported task interdependence. At the 95% confidence level, survey participants from organizations with 15,000 or more employees reported significantly higher levels of task interdependence compared to participants from organizations with less than 2,500 employees. Second, participants in managerial positions reported significantly higher levels of task interdependence compared to participants in technical jobs. Third, in general, the more information technology experience the participant had, the higher the reported task interdependence. Participants with more than 15 years of IT experience reported significantly higher levels of task interdependence compared to participants with less than 8 years of IT experience. The second and third findings are related in that the more IT experience a person has the more likely the person will be in a managerial position. Fourth, participants from organizations with a dedicated security office reported significantly higher levels of task interdependence compared to participants from organizations without a dedicated security office. Fifth, participants from organizations with a top security officer (e.g. chief security officer) reported significantly higher task interdependence compared to participants from organizations without a top security officer. The fourth and fifth findings are related in that organizations with a dedicated security office are likely to have a dedicated security officer. In addition, the first, fourth, and fifth findings are related in that larger organizations are more likely to have dedicated security departments with a permanent top security officer than smaller organizations since larger organizations have more resources to secure.

Analyzing demographics based on environmental factors provided in Figure 2 revealed few significant differences at the 95% confidence level. At the country level, respondents from Singapore reported significantly lower levels of task interdependence compared to respondents from the U.S., Canada, and the U.K. Yet, country results should be interpreted carefully since diverse cultures may define task interdependence differently. For example, Singaporean culture and their view of individualism and teamwork [22] may affect how participants conceptualize task interdependence. Also, respondents in the education and IT/Telecommunication sectors had significantly lower levels of reported task interdependence than respondents in the utilities sector. The higher ratings from participants in the utilities sector may be due in part to recent governmental regulation and societal attention. For example, since September 2001, there has been increased attention to share information in sectors that operate critical infrastructures [23] including power and communication utilities. Increased information sharing dictated by government or industry regulation could have motivated the higher task interdependence scores from participants working in utilities. In other demographics, the lower sample sizes from both the country and sector sub-samples may have prevented significant differences from arising. The Appendix provides full demographic information.

5. Discussion

The results from the two scales suggest that information security work in organizations exhibits high levels of task interdependence. Four findings in particular suggest support for the proposition of this paper. First, the qualitative responses provided initial evidence that organizational cooperation is critical to achieve information security goals. Second, based on the results of using the Pearce et al scale, information security received a high rating in task interdependence compared to the other IS tasks listed in the Sharma & Yetton meta-analysis. Third, the 936 respondents who completed the Van de Vegt et al scale indicated an average of 62% of their daily tasks require the exchange of information or cooperation with others. Fourth, based on a comparison of results in the associated article [13], information security has nearly twice the measure of task interdependence compared to telecommunications software development.

Based on the findings of this exploratory study, we argue that information security work in organizations demonstrates high levels of task interdependence. If this indeed is the case, what then makes information security work so interdependent? Readers may recognize the saying that *security is everyone's business*. In fact, a web search revealed hundreds of uses of this common phrase. While many organizations hire certified professionals to lead security programs, information security practices must include every employee who handles sensitive or privileged information. In modern organizations where technology is ubiquitous and privileged information routinely automated, security, out of necessity, requires a team effort and organizational cooperation. Based on our reading of the qualitative

Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07)
0-7695-2755-8/07 $20.00 © 2007 IEEE

responses, the interdependent nature of security seems to apply across information security tasks. While our study did not specifically investigate which areas within information security require the most interdependence, we did find evidence that task interdependence is important in diverse areas of information security such as network architecture, application security, human resource security, physical security, operations security and business continuity management. Thus, we suggest that information security work in general exhibits high task interdependence.

5.1. Directions for Future Research

The results of this study provide preliminary evidence that information security-related work requires high levels of task interdependence. This finding has ramifications for the IS researcher by identifying new areas for study. A review of the literature revealed a number of promising research topics. We list five research areas from the literature that each could be extended to information security.

First, high levels of task interdependence require greater instances of information exchange needed to clarify task assignments, project requirements, and progress [18]. In the context of the Andres & Zmud study, the authors found partial support in a software development environment that low task interdependence will lead to more successful projects than high task interdependence. Thus, high task interdependence environments can be difficult and require greater levels of communication than low environments. The study also found that organic coordination can afford greater productivity than mechanistic coordination especially in high task interdependent software development environments. Organic coordination is associated with informal, cooperative, and decentralized strategies whereas mechanistic coordination is associated with formal, controlling, and centralized strategies. In high task interdependence environments, the role of top management in performing clarifying tasks may be critical to success. If, like high task interdependence software development environments, information security also requires greater levels of coordination, it would be useful to know which type is more effective (i.e. organic or mechanistic). This subject seems highly relevant to information security and researchers may be able to extend the Andres & Zmud findings in future studies.

Second, the effects of peer monitoring have been demonstrated to positively affect employee performance in high-task interdependency environments. Peer monitoring can encourage coworkers to perform better when peers notice and respond to their coworkers behaviors. In one study of theme park work, constructive peer monitoring was beneficial particularly in environments of high task interdependence and low supervision [24]. Organizations with cultures that embrace security may also benefit from peer monitoring as a means of enforcing security policies. Many participants in our study mentioned the use of network-based monitoring tools to help with policy enforcement. Future investigations could examine the usefulness of peer-based monitoring as a part of a balanced monitoring program that includes network-based monitoring [25].

Third, dissimilar educational levels on multidisciplinary teams may be important factors to consider in determining how supervisors could change the level of task interdependence by altering the distribution of individual tasks within a team [13]. This may have research implications in the area of information security policy considering that policy development teams may include members from across an organization where educational levels are dissimilar. Our study suggests information security environments in general will be high in task interdependence. However, supervisors may be able to exercise some flexibility by considering the educational backgrounds of individuals when assigning security tasks and responsibilities.

Fourth, organizational citizenship behavior (OCB), which helps describe the extent to which employees go above and beyond to contribute to collective success [26], may be particularly appropriate for tasks high in interdependence. One study found that in high task interdependence conditions, OCB ratings appeared higher than in low task interdependence conditions [27]. The concept of citizenship and the application of OCB to information security seems especially relevant for future research. Perhaps the goal of security training and awareness programs is to cultivate employee loyalty where security rules are not merely tolerated, but employees take it upon themselves to be good organizational security citizens.

Fifth, researchers can explore the relationships between task interdependence and information security and the computer-supported collaborative work (CSCW) literature. In a CSCW field study investigating intrusion detection work, researchers found significant levels of distributed collaboration. Especially in larger organizations, “analysts tended to work in groups. The members of these groups shared the workload of intrusion detection and collaborated on different problems” [28, p. 344]. The authors concluded that information security through intrusion

detection, "is richly collaborative both in the learning strategies and in the mundane and exceptional performance of the work" [28, p. 345]. Thus, the conclusions of this CSCW study into the intrusion detection area of information security yielded similar results to the current study involving task interdependence. Future studies can further explore different areas of information security as it applies to CSCW as well as task interdependence.

In review, each of the above five topics and others in the task interdependence literature can be extended to future studies in information security. We encourage researchers to explore the task interdependence literature for other possible topics that may apply to information security.

5.2. Implications for Practice

Previous studies suggest that organizational work high in task interdependence requires greater levels of executive support to be successful [15]. Executive support has been significantly linked to important information security constructs such as policy enforcement and organizational security culture [29]. Identifying information security as a task high in interdependence helps practitioners understand why executive support is critical to ensuring security effectiveness. Without this support, security programs may not get the organizational-wide cooperation needed to be successful. Considering the importance of information security to the modern organization, additional insight into the nature of information security as work requiring high levels of cooperation and teamwork will help practitioners improve upon the management of their programs and thus better protect information.

5.3. Study Limitations

While the combined qualitative and quantitative results provide convincing evidence in favor of the proposition, we must recognize limitations of this exploratory study. Comparing our results to a survey that used the same instrument but on different populations must be interpreted with some caution. For example, our worldwide sample exclusively involved information security professionals where the Netherlands sample using the Van der Vegt scale involved 20 multidisciplinary software development teams. Future studies can investigate this topic using confirmatory methods where comparisons use samples that are more homogeneous such as surveying differences in task interdependence between various IT jobs within a single organization. Additionally, our sample was limited to one information security-certifying constituency. Surveying other constituencies or non-certified information security workers may yield different results than surveying CISSPs. Also, we must be cognizant of the bias in the information security worker population. The empirical results in our study are taken from information security professionals; one can argue that they see inflated interdependencies in their own work. In sum, our data allowed tentative findings regarding levels of task interdependence in information security work. Future research comparing levels of task interdependence with other IT-related tasks is warranted.

6. Conclusion

We believe that the notion of task interdependence is a meaningful and useful concept to help researchers and practitioners alike understand the nature of information security work in organizations. Future research can further investigate information security, task interdependence and related topics such as organizational citizenship behavior. Considering the critical nature of information security to modern society, additional insight into the interdependent and cooperative nature of this area is needed. As Mary Ann Davidson, Chief Security Officer of the Oracle Corporation stated, "A major cultural shift needs to occur in the enterprise. Security is not merely the firewall administrator's job or the gate guard's job or the security administrator's job. Everyone needs to be good security citizens, or they run the risk of subjecting themselves, as well as their colleagues, to vulnerabilities" [30].

7. Acknowledgments

The authors gratefully thank Dorsey Morrow and the (ISC)^2 organization for their support during this project as well as the four anonymous reviewers for their helpful insights.

8. References

[1] C. D. Schou and K. J. Trimmer, "Information Assurance and Security," *Journal of Organizational and End User Computing*, vol. 16, pp. i-vii, 2004.
[2] D. G. Blankinship, "Hotels.com Customer Info May Be At Risk," June 3 ed: Business Week Online, 2006.
[3] D. Kaplan, "Twelve Firefox Flaws Fixed," vol. June 5: SC Magazine, 2006.
[4] K. Bagchi and G. Udo, "An Analysis of the Growth of Computer and Internet Security Breaches," *Communications of the AIS*, vol. 12, pp. 684-700, 2003.

[5] L. A. Gordon, M. P. Loeb, W. Lucyshyn, and R. Richardson, "10th Annual CSI/FBI Computer Crime and Security Survey," Computer Security Institute, San Francisco, CA 2005.
[6] A. Garg, J. Curtis, and H. Halper, "The Financial Impact of IT Security Breaches: What Do Investors Think?," *Information Systems Security*, vol. 12, pp. 22-34, 2003.
[7] G. Dhillon and J. Backhouse, "Current Directions in IS Security Research: Towards Socio-organizational Perspectives," *Information Systems Journal*, vol. 11, pp. 127-153, 2001.
[8] A. G. Kotulic and J. G. Clark, "Why There Aren't More Information Security Research Studies," *Information & Management*, vol. 41, pp. 597-607, 2004.
[9] M. E. Whitman and H. J. Mattord, *Management of Information Security*. Cambridge, MA: Course Technology - Thompson Learning, 2004.
[10] D. B. Parker, *Computer Security Management*. Reston, Virginia: Reston Publishing Company, 1981.
[11] NSTISS, "National Training Program for Information Security Professionals," Available at http://www.cnss.gov/directives.html NSTISSD No. 501, November 16 1992.
[12] ISO/IEC, "Information Technology - Code of practice for information security management," The International Standards Organization/The International Electrotechnical Commission ISO/IEC 17799:2000(E), December 2000.
[13] G. S. Van der Vegt, E. Van de Vliert, and A. Oosterhof, "Informational Dissimilarity and Organizational Citizenship Behavior: The Role of Intrateam Interdependence and Team Identification," *Academy of Management Journal*, vol. 46, pp. 715-727, 2003.
[14] J. D. Thompson, *Organizations in Action*. New York: McGraw Hill, 1967.
[15] R. Sharma and P. Yetton, "The Contingent Effects of Management Support and Task Interdependence on Successful Information Systems Implementation," *MIS Quarterly*, vol. 27, pp. 533-555, 2003.
[16] W. Orlikowski, "The Duality of Technology: Rethinking the Concept of Technology in Organizations," *Organization Science*, vol. 3, pp. 398-427, 1992.
[17] M. B. Stanne, D. W. Johnson, and R. T. Johnson, "Does Competition Enhance or Inhibit Motor Performance: A Meta-Analysis," *Psychological Bulletin*, vol. 125, pp. 133-154, 1999.
[18] H. P. Andres and R. W. Zmud, "A Contingency Approach to Software Project Coordination," *Journal of Management Information Systems*, vol. 18, pp. 41-70, 2003.
[19] B. S. Collins and S. Mathews, "Securing Your Business Processes," *Computers & Security*, vol. 12, pp. 629-633, 1993.
[20] C. C. Wood, "Why Information Security is Now Multi-disciplinary, Multi-departmental, and Multi-organizational in Nature," *Computer Fraud & Security*, vol. 2004, pp. 16-17, 2004.
[21] J. L. Pearce, S. M. Sommer, A. Morris, and M. Frideger, "A Configurational Approach to Interpersonal Relations: Profiles of Workplace Social Relations and Task Interdependence (Working Paper GSM #OB92015)," University of California, Irvine, 1992.
[22] S. McCoy, D. F. Galletta, and W. King, R., "Integrating National Culture Into IS Research: The Need for Current Individual-Level Measures," *Communications of the Association for Information Systems*, vol. 15, pp. 211-224, 2005.
[23] 9/11 Commission, *The 9/11 Commission Report - Final Report of the National Commission on Terrorist Attacks Upon the United States*, Authorized, First ed. New York: W. W. Norton & Company, 2004.
[24] M. L. Loughry, "Coworkers are Watching: Performance Implications of Peer Monitoring," presented at Academy of Management Conference, Hammersmith, London, 2002.
[25] J. F. George, "Computer-Based Monitoring: Common Perceptions and Empirical Results," *MIS Quarterly*, vol. 20, pp. 459-480, 1996.
[26] D. W. Organ, *Organizational Citizenship Behavior: The Good Soldier Syndrome*. Lexington MA: Lexington Books, 1988.
[27] D. G. Bachrach, B. C. Powell, E. Bendoly, and R. G. Richey, "Organizational Citizenship Behavior and Performance Evaluations: Exploring the Impact of Task Interdependence," *Journal of Applied Psychology*, vol. 91, pp. 193-201, 2006.
[28] J. R. Goodall, W. Lutters, G., and A. Komlodi, "I Know My Network: Collaboration and Expertise in Intrusion Detection," presented at ACM Conference on Computer Supported Cooperative Work (CSCW), Chicago, Illinois, 2004.
[29] K. J. Knapp, T. E. Marshall, R. K. Rainer, Jr., and F. N. Ford, "Information Security: Management's Effect on Culture and Policy," *Information Management & Computer Security*, vol. 14, pp. 24-36, 2006.
[30] M. Savage, "Time to Act: New Challenges in 2004," vol. December 1: SC Magazine, 2003.

Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07)
0-7695-2755-8/07 $20.00 © 2007 IEEE

Appendix. Task Interdependence Results by Demographic. Note: Some of the smallest sub-samples (e.g. n < 10) are not listed.

	n	Mean	S.D.	Lower 95% C.I.	Upper 95% C.I.
Country:					
Netherlands	18	3.44	0.46	3.22	3.67
UK	44	3.78	0.59	3.60	3.96
Australia & New Zealand	29	3.69	0.63	3.45	3.93
Canada	73	3.68	0.53	3.55	3.80
Hong Kong	27	3.67	0.64	3.42	3.92
USA	514	3.61	0.65	3.55	3.66
India	24	3.48	0.58	3.23	3.72
Singapore	25	3.21	0.69	2.92	3.49
Number of Employees:					
less than 500	231	3.41	0.69	3.33	3.50
Between 500 and 2,499	160	3.49	0.64	3.39	3.59
Between 2,500 and 7,499	142	3.58	0.63	3.47	3.68
Between 7,500 and 14,999	79	3.63	0.68	3.48	3.78
greater than 15,000	323	3.68	0.63	3.61	3.75
Sector (Respondents were free to select multiple sectors):					
Utilities	32	3.82	0.53	3.63	4.01
Energy	28	3.64	0.65	3.39	3.89
Travel, Hospitality	13	3.64	0.75	3.18	4.09
Manufacturing	82	3.64	0.63	3.50	3.77
Professional Services (Legal, Marketing, etc.)	42	3.63	0.54	3.46	3.80
Government - federal, local, military, etc.	217	3.62	0.64	3.54	3.71
Industrial Technology	22	3.62	0.80	3.26	3.97
Finance, Banking, Insurance	238	3.59	0.64	3.51	3.67
Healthcare, Medical	80	3.59	0.63	3.45	3.73
Retail, Consumer Products, Wholesale	56	3.54	0.56	3.39	3.69
Transportation, Warehousing	20	3.53	0.81	3.15	3.91
Information Technology, Telecommunications	254	3.52	0.69	3.44	3.61
Non-Profit	14	3.42	0.51	3.13	3.72
Education	60	3.41	0.71	3.22	3.59
Does the organization have a top security position (e.g. CSO, CISO)?					
Yes	585	3.63	0.65	3.58	3.69
No	332	3.43	0.65	3.36	3.50
Does the organization have a dedicated office responsible for security issues?					
Yes	760	3.61	0.65	3.56	3.66
No	170	3.35	0.65	3.25	3.45
Job Type:					
Technical	716	3.52	0.66	3.47	3.57
Managerial	217	3.71	0.63	3.63	3.79
IT-experience of respondent:					
less than 8 years	224	3.41	0.69	3.32	3.50
Between 8 and 15 years	411	3.58	0.63	3.52	3.64
greater than 15 years	299	3.65	0.65	3.57	3.72