Journal of Business Studies Quarterly
2014, Volume 6, Number 1 ISSN 2152-1034

Journal of Business Studies Quarterly jbsq.org

THE INFLUENCE OF INFORMATION SYSTEMS SECURITY ON JOB PERFORMANCE: A PROPOSED RESEARCH TOPIC

Irikefe Urhuogo
Argosy University
College of Business and Information Technology
iurhuogo@stu.argosy.edu

Archie Addo
Argosy University
College of Business and Information Technology
aaddo@.argosy.edu

Dorothy Williams
Argosy University
College of Business and Information Technology
djwilliams@.argosy.edu

Abstract

The paper proposed a potential research topic on Information systems' (IS) security influences on users' work performance. IS researchers have discussed security measures and the types of IS security implemented in organizations. Nevertheless, little has been said about the impact of IS security on users' work performance. This paper uses the system development life cycle (SDLC) to determine how the type of security systems implemented in organizations can affect employees' work performance. The research questions asked: How does the IS security system used in an organization affect users' work performance? Is the IS security system strong enough to secure employees' and customers' data? A qualitative research design will be used to gather the data.

Keywords: IS, Security, Users, Work Performance.

1. Introduction

Understanding information system (IS) security implementation in an organization has proven to be difficult. It is even more complicated to determine if an organization's security system has the potential of improving employees' job performance. IS security and organizations' performance has been studied by IS researchers (Chen, Ramamurthy, & Wen, 2012; Guo, Yuan, Archer, & Connelly, 2011). As organizational management thrives to implement appropriate security measures in their organization, they may neglect to consider the impact of the IS security on employees' work performance. Appropriate IS security protocols can potentially improve employees' various work responsibilities if the protocols are understood by employees. For instance, employees are likely to improve their work performance if they implement IS security protocols accurately to different areas of their work. While appropriate IS security measures can potentially improve work performance, they can also decrease users' work performance if the security system permits them to access confidential information that does not pertains to their work responsibilities. Researchers have mentioned the need for adopting IS that would be easy to understand, the effect of IS users' participation in security controls, and the importance of drafting security control polices and guidelines for employees to follow (Gebauer, 2008; Spears & Barki, 2010; Siponen & Vance, 2010). Despite all that has been said about IS security, mainstream research has paid little attention to the impact of an organization's IS security on an individual level. Thus, the goal of this paper is to investigate the impact of IS security on work performance using the system development life cycle (SDLC) and a qualitative research approach.

The current research contributes to several streams in IS literature by highlighting the significance of IS security professionals and manufactures to build systems that enable organizations to meet their objectives. The results of this proposed research topic might be applied to improve the manner in which organizational management contemplate which security systems to implement in their organization. This study contributes to the field of business because there is limited knowledge in the literature regarding the effectiveness of organization's security systems on employees' work performance. Professionals in the field of business may use the results to better understand which type of features and functions to build into IS security and implement security standards and protocols that would enable users to adhere to systems security. Hence, professionals may be able to use the information to develop IS security training programs for users in various organizations. The ability to manage an organization's data is indicative of the credibility and capability of the organization to manage employees' and customers' data. Therefore, this research topic is significant because it would provide management with insights on how they can improve employee work performance based on the type of IS that are introduced in their organization, and how to choose appropriate systems that will suit their various business objectives (Srivastava & Teo, 2012).

The paper is organized into eight sections. The second section provides a background information on the influence of IS security on users' work performance. The third section discusses the problem statement of IS security influence on employees' work performance. The fourth section mentions the purpose of the research. The fifth section discuses the theoretical perspective employed. The sixth section describes the methodology procedures for gathering information. The seventh section discusses the proposed instrumentation used to gather the data. The eighth section contains the conclusion.

2. Background

Due to the use of a variety of technological equipment in organizations, management has implemented security measures in order to protect their organization's proprietary information. To protect confidential information, organizational management outsources their security protection to organizations that specialize in IS security. Hui, Hui, and Yue (2012) observed that outsourcing IS security to a third party organization may has its benefit. However, outsourcing IS security can negatively affect the social welfare of an organization if the organization's information is not adequately protected. For instance, multiple organizations that outsource their security protection services to the same provider may encounter greater system interdependency risks. Furthermore, contemplating the impact of security countermeasures, Kumar, Park, and Subramaniam (2008) noted that when organizational management make decisions about new security countermeasures, they sometimes add advanced security protection to existing security measures. Thus, a previous security system together with an advance one can potentially assist an organization in achieving its goals. The ability of an organization to achieve its objectives are indicative that employees work performance can potentially be improved.

Management should ensure that security measures improve users' work performance as they implements appropriate IS security measures in their organization. A study conducted by Erickson and Jacoby (2003) revealed that when management participate in different networks that are affiliated with their organization, employees are more likely to have high-performance work practices and participate in employee training programs. When different IS security training programs are introduced in organizations, management can use the training medium to test the effectiveness of the training programs to ensure they achieved their intended purposes. Employees can improve their various work responsibilities if the IS security system is strong enough to manage the various data they use on a regular basis. Reflecting on the effect of systems security, Chen, Kataria, and Krishnan (2011) observed that even though systems vulnerability can affect the confidentiality, integrity, and availability of organizational information, an appropriate encoding protocol can protect an organization's privacy and integrity of information. Ko et al. (2012) noted that effective systems can result in better control of customers' information, access to confidential information, control of system access, and retrieval of data.

Current studies have discussed IS research from different perspectives. For instance, empirical research has noted the importance of IS users to employ an organization's system effectively (Deng, Chi, 2012). Further research reflect the importance of organizational management to constantly revise the manner in which their employees use the organization's IS (Sun, 2012), and how employees' use of an organization IS can affect the benefit of the system to the organization (Venkatesh, Brown, Maruping, & Bala, 2008). Additional research have noted the impact of IS security on system standards(Hui, Hui, & Yue, 2012), the manner in which management of organizations manages their IS security (Johnston & Hale, 2009), the importance of IS security in individual homes (Denning, Tadayoshi, & Levy, 2013), the impact of IS breaches in organizations (Gordon, Loeb, & Lei, 201), different strategies management can use to secure their organization's personal information (Jae-Gu, Gil-Cheol, & Seoksoo, 2007), and the risks involved in IS security management (Bodin, Gordon, & Loeb, 2008).

When employees are unfamiliar about how to apply their organization's security system to their different job responsibilities, they inadvertently neglect to achieve all aspects of their organization's objectives. As a result, lack of proper adoption negatively affects their job performance. Miller and Doyle (1987) stated that organizations that have high work performance are those that implement IS that matches their organization's goals and visions and that are easy to adopt. Because IS security can have different functions in organizations, management should ensure that the IS their organization utilizes is effective and suits the organization's objectives.

3. Problem Statement

The problem being addressed in this study is that there is little research on the impact of IS security on employees' work performance. The literature on IS use is diverse. Empirical research has noted the importance of IS users to employ an organization's system effectively (Deng, Chi, 2012), the importance of organizational management to constantly revise the manner in which their employees use the organization's IS (Sun, 2012), how employees' use of an organization IS can affect the benefit of the system to the organization (Mahmood & Becker, 1985), the importance of users' satisfaction with the systems they use in their organization (Doll, Xiaodong, Raghunathan, Torkzadeh, & Weidong, 2004), and IS users resistance to organization's different system implementation (Kim & Kankanhalli, 2009).

Other researchers have noted the impact of IS security on system standards, the manner in which management of organizations manages their IS security(Hui, Hui, & Yue, 2012), the importance of IS security in individual homes (Johnston & Hale, 2009), the impact of IS breaches in organizations (Denning, Tadayoshi, & Levy, 2013), different strategies management can use to secure their organization's personal information (Gordon, Loeb, & Lei, 2011), and the risks involved in IS security management(Jae-Gu, Gil-Cheol, & Seoksoo, 2007). While the various studies contributed significantly to understanding IS security influence on organization, there is still the need to explore the influence of IS security influence on end users' work performance.

4. Purpose of Research

The purpose of the study is to investigate the influence of IS security on employees' work performance. While employees' adoption of their organizations IS security system is important, their ability to use the system to improve their work performance is important as well.

5. Theoretical Framework

The theoretical framework chosen for this research is the system development life cycle (SDLC). The SDLC originated in the 1960s and held that in order for IS manufacturers to build effective systems, they must follow certain steps (Lai & Tsen, 2013). These steps are project planning, feasibility study, systems analysis, systems design, implementation and integration, acceptance and installation, deployment and maintenance, and disposal (Pollard, Gupta, &

Satzinger, 2010; Lai & Tsen, 2013). Organizational management should consider various IS that would enable them to test the effectiveness of the IS before implementing the system (Taneja, Golden Pryor, Humphreys, & Pryor Singleton, 2013). To ensure that the IS achieve their intended purposes, management should collaborate with IS manufacturers so that the IS used in their organization will be customized accordingly.

6. Research Methodology

6.1. Research Design

A qualitative research, in the form of an interview, will be used to gather data for this study. A qualitative research provides an in-depth understanding of a research topic (Clark, 2009). For instance, instead of asking participants to provide a *yes* or *no* response to questions, participants are given the opportunities to provide a detailed explanation for each question. The detailed explanation will give the researchers a better understanding of the responses given. Some reasons for asking personal questions are because this type of research approach "assumes that human…behavior is seen to be influenced by many factors, including values, beliefs, knowledge, cultural background, relationships with others, social norms, and aspirations" (Clark, 2009, p. 132). During the interview, participants will be asked to describe how they feel about IS security implementation, and how the security system used in their organization has impacted their various job responsibilities.

6.2. Research Trustworthiness

To ensure that the data derived during qualitative inquiry is valid, researchers must establish the trustworthiness of the qualitative research. Establishing the trustworthiness of a qualitative research involves enhancing the credibility, transferability, dependability, and conformability of the research (Whiting & Sines, 2012). Enhancing the credibility of research will require researchers to be persistent observers, meaning they will need to dedicate a significant amount of time in observing participants' behaviors. Credibility requires researchers to conduct studies in a manner that will be believable by other researchers (Houghton, Casey, Shaw, & Murphy, 2013). To ensure that the researcher did not miss anything during the observation, he or she should invite other researchers who are involved in the research to conduct member-checking to ensure information is transcribed accurately. Also, if researchers choose to use a qualitative research approach to gathering their data regarding the effectiveness of different IS in managing organization's data, they must interview key employees who use special software in the organization. Thus, participants will be interviewed for this study.

6.3. Research Questions

RQ1- How does the IS security system used in an organization affect end-users' work performance?

RQ2- Is the IS security system strong enough to secure employees and customers' information?

6.4. Participants

The researcher will interview ten participants in the study. These participants will be randomly selected from an organization in the health care industry. This organization is chosen because the organizational management recently implemented a security system in their organization and was not certain if the system has a positive effect in employees' work performance. The participants chosen for this research uses the organization security system on a daily basis and is familiar with the system procedures. The participants belong to Hispanic, Caucasian, African American, and Native Americans races and the researcher is not affiliated with any of the participants who will be involved in the research.

6.5. Interview

Before embarking on the interview, the researcher will ensure that the environment in which the interview will be conducted does not have any conflicting variables or factors that can affect the validity of the study (Mitchell, 2011; Brédart, Marrel, Abetz-Webb, Lasch, & Acquadro, 2014). For instance, interview rooms will be secure to avoid outside distractions, and the researcher will prepare the interview rooms before conducting any interview (Brédart, Marrel, Abetz-Webb, Lasch, & Acquadro, 2014). Bansal and Corley (2012) noted that qualitative research "has considerable latitude in their methods, including the way in which researchers conduct interviews or ethnographies and the techniques they use to analyze data" (p. 511). Conflict of interest will be avoided by ensuring that a five minutes window is provided for each interview so that the participants do not discuss their interview with each other before the interview sessions. The researcher of the proposed research topic will use different data technique, such as coding, to analyze the data. During the interview, participants will be asked to describe how the organization's security system affects their various work responsibilities.

7. Instrumentation

The qualitative instrument will be developed by the researcher. The instrument contains three categorical questions that ask participants to describe how their organization's system security influence their job performances, if the security system is strong enough to protect employees and customers' data, and how they think their organization's security system can be improved. The first section of the instrument will asked participants to provide general information such as their age, sex, and race. The second section will contain questions that pertain to the use of their organization security system. The researcher will record the interview and an interview protocol developed by the researcher will be used to gather the data. The interview will last between 45-50 minutes per person. The interview room will contain two chairs, one for the interviewer and one for the interviewee. Before the interview begins, the researcher will inform the participants of the type of questions they will be asked and that they are expected to provide short and detailed responses to the best of their abilities. Participants will be asked open-ended and close-ended questions and the researcher will approach all interviews in like manner. There are no foreseen risks associated with the interview and participants will complete a letter of consent stating that their involvement in the study is voluntary. To enhance confidentiality, aliases will be used to identify the participants in the study. The information collected during the interview will be kept in a locked cabinet to which the researcher is the only person who has the key.

8. Conclusion

There are many IS security available in which employees may find difficult to adapt to the in their organization. As a result, IS security training programs are introduced in organizations to monitor, evaluate, and measured employees' work performances. Miller and Doyle (1987) indicated that organizations with high work performance efficaciously achieved their organization's goals and visions. This research proposal identifies the need for further research on the influence of security systems on employees' work performance, using the SDLC framework.

References

Bansal, P., & Corley, K. (2012). What's different about qualitative research? *Academy of Management Journal*, 509-513.

Bodin, L. D., Gordon, L. A., & Loeb, M. P. (2008). Information security and risk management. *Communications of the ACM*, *51*(4), 64-68.

Brédart, A., Marrel, A., Abetz-Webb, L., Lasch, K., & Acquadro, C. (2014). Interviewing to develop Patient-Reported Outcome (PRO) measures for clinical research: Eliciting patients' experience. *Health & Quality Of Life Outcomes*, *12*(1), 1-20.

Chen, Y., Ramamurthy, K. K., & Wen, K. (2012). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems*, *29*(3), 157-188.

Chen, P., Kataria, G., & Krishnan, R. (2011). Correlated failures, diversification, and information security risk management. *MIS Quarterly*, *35*(2), 397-A3.

Clark, A. M. (2009). Qualitative research: What it is and what it can contribute to cardiology in the young. *Cardiology in the Young*, 131-134.

Deng, X., & Chi, L. (2012). Understanding postadoptive behaviors in information systems use: A longitudinal analysis of system use problems in the business intelligence context. *Journal of Management Information Systems*, *29*(3), 291-326

Denning, T., Tadayoshi, K., & Levy, H. M. (2013). Computer security and the modern home. *Communications of The ACM, 56*(1), 94-103.

Doll, W. J., Xiaodong, D., Raghunathan, T. S., Torkzadeh, G., & Weidong, X. (2004). The meaning and measurement of user satisfaction: A multigroup invariance analysis of the end-user computing satisfaction instrument. *Journal of Management Information Systems*, *21*(1), 227-262.

Erickson, C. L., & Jacoby, S. M. (2003). The effect of employer networks on workplace innovation and training. *Industrial & Labor Relations Review*, *56*(2), 203-223.

Frels, R. K., & Onwuegbuzie, A. J. (2013). Administering quantitative instruments with qualitative interviews: A mixed research approach. *Journal of Counseling & Development*, *91*(2), 184-194.

Gebauer, J. (2008). User requirements of mobile technology: A summary of research results.

Information Knowledge Systems Management, *7*(1/2), 101-119.

Gordon, L. A., Loeb, M. P., & Lei, Z. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security*, *19*(1), 33-56.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems*, *28*(2), 203-236.

Hoe, J., & Hoare, Z. (2012). Understanding quantitative research: Part 1. *Nursing Standard*, *27*(15-17), 52-57.

Houghton, C., Casey, D., Shaw, D., & Murphy, K. (2013). Rigour in qualitative case-study research. *Nurse Researcher*, *20*(4), 12-17.

Hui, K., Hui, W., & Yue, W. T. (2012). Information security outsourcing with system interdependency and mandatory security requirement. *Journal of Management Information Systems*, *29*(3), 117-156.

Jae-Gu, S., Gil-Cheol, P., & Seoksoo, K. (2007). RFID based context information security system architecture for securing personal information under ubiquitous environment. *AIP Conference Proceedings*, *963*(2), 563-566.

Johnston, A. C., & Hale, R. (2009). Improved security through information security governance. *Communications of The ACM*, *52*(1), 126-129.

Kim, H., & Kankanhalli, A. (2009). Investigating user resistance to information systems implementation: A status quo bias perspective. *MIS Quarterly*, *33*(3), 567-582.

Kisely, S., & Kendall, E. (2011). Critically appraising qualitative research: A guide for clinicians more familiar with quantitative techniques. *Australasian Psychiatry*, *19*(4), 364-367.

Kumar, R. L., Park, S., & Subramaniam, C. (2008). Understanding the value of countermeasure portfolios in information systems security. *Journal of Management Information Systems*, *25*(2), 241-279.

Lai, W., & Tsen, H. (2013). Exploring the relationship between system development life cycle and knowledge accumulation in Taiwan's IT industry. *Expert Systems*, *30*(2), 173-182.

Mahmood, M. O., & Becker, J. D. (1985). Effect of organizational maturity on end-users' satisfaction with information systems. *Journal of Management Information Systems*, *2*(3), 37-64.

Miller, J. J., & Doyle, B. A. (1987). Measuring the effectiveness of computer-based information systems in the financial services sector. *MIS Quarterly*, *11*(1), 107-124.

Mitchell, M. (2011). A reflection on the emotional potential of qualitative interviewing. *British Journal of Midwifery*, *19*(10), 653-657.

Pollard, C. E., Gupta, D., & Satzinger, J. W. (2010). Teaching systems development: A compelling case for integrating the SDLC with the ITSM Lifecycle. *Information Systems Management*, *27*(2), 113-122.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, *34*(3), 487-A12.

Srivastava, S. C., & Teo, T. H. (2012). Contract performance in offshore systems development: Role of control mechanisms. *Journal of Management Information Systems*, *29*(1), 115-158

Sun, H. (2012). Understanding user revisions when using information system features: Adaptive system use and triggers. *MIS Quarterly*, *36*(2), 453-478

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly*, *34*(3), 503-A5.

Taneja, S., Golden Pryor, M., Humphreys, J. H., & Pryor Singleton, L. (2013). Strategic management in an era of paradigmatic chaos: Lessons for managers. *International Journal of Management*, *30*(1), 112-126

Venkatesh, V., Brown, S. A., Maruping, L. M., & Bala, H. (2008). Predicting different conceptualizations of system use: The competing roles of behavioral intention, facilitating conditions, and behavioral expectation. *MIS Quarterly*, *32*(3), 483-502.

Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quarterly*, *37*(1), 21-54

Whiting, M., & Sines, D. (2012). Mind maps: Establishing 'trustworthiness' in qualitative research. *Nurse Researcher*, *20*(1), 21-27.