Winter 12-10-2016

Too Much of a Good Thing? An Investigation of the Negative Consequences of Information Security in a Healthcare Setting

Azadeh Savoli
IESEG School of Management, a.savoli@ieseg.fr

Shamel Addas
Queen's University, shamel.addas@queensu.ca

Isabelle Fagnot
Audencia, ifagnot@audencia.com

Too Much of a Good Thing? An Investigation of the Negative Consequences of Information Security in a Healthcare Setting

Research in Progress

Azadeh Savoli
IESEG School of Management, France {a.savoli@ieseg.fr}

Shamel Addas
Queen’s University, Canada {shamel.addas@queensu.ca}

Isabelle Fagnot
Audencia Business School, France {ifagnot@audencia.com}

ABSTRACT

Information security is becoming a prime concern for individuals and organizations. This is especially true in healthcare settings where widespread adoption of integrated health information systems means that a vast amount of highly sensitive information on patients is accessible through many interaction points across the care delivery network.

In this research in progress, we seek to uncover how individuals react when they perceive that their security environment is stressful. To do so, we conducted a case study using an inductive approach based on semi-structured interviews with 41 participants. The preliminary analysis of some of our interviews showed that too much security in a health setting can bring in negative consequences like evoking negative emotions in users toward the system, increased dissatisfaction, and increase of inappropriate workarounds, which can lead to ineffective usage of the system and eventually can put patients’ health at risk.

Keywords: Patients’ health information, information security, health information systems, qualitative research.

INTRODUCTION

In today’s increasingly digital business environment, information security is becoming a prime concern for individuals and organizations. This is especially true in healthcare settings where widespread adoption of integrated health information systems means that a vast amount of highly sensitive information on patients is accessible through many interaction points across the care delivery network. Indeed, such widespread access has facilitated and dramatically intensified security violations from potential harmers, both intended and unintended (Stahl et al. 2012). It is estimated that the legal settlements alone arising from security violations and issues cost the US healthcare sector over $6 billion per year (Appari & Johnson 2010).

Because people are the weakest link in fending off such security threats (Lowry & Moody 2015), organizations are increasingly investing in security mechanisms and policies that encourage security compliance. Not surprisingly, this has spawned a vast area of research aimed at uncovering the factors that influence compliance intentions and behaviors among individuals. Studies have focused on antecedent factors of compliance (Straub 1990; von Solms & von Solms 2004; Warkentin et al. 2006), non-compliance (e.g., Hu et al. 2011; Myyry et al. 2009; Siponen & Vance 2010;), or both (Lowry & Moody 2015). Common across these studies is an implicit assumption that increased security is always beneficial. However, it is possible that individuals who perceive their security environment to be taxing would react in ways that undermine the organization's intended security goals. While this notion that implementing security policies can trigger negative consequences has received some support (e.g., d'Arcy et al. 2014), our understanding of how individuals react when they perceive security to be a burden remains quite limited. In particular, little is known about the emotional, cognitive, and behavioral consequences and interactions between these factors. Therefore, our research question is: *How do individuals react to a stressful IS security environment?* We conceptualize a stressful security environment as one where there is a misfit between the characteristics of the person and the environment (Cooper et al. 2001). This can occur when the security environment creates unmet personal needs or preferences, or when it creates demands that exceed personal abilities. Our research setting is the healthcare sector.

BACKGROUND

It is widely agreed that IS security extends beyond technical aspects (Stahl et al. 2012). Following Dhillon & Torkzadeh (2006), we define IS security as "the protection of information resources of a firm, where such protection could be through both technical means and by establishing adequate procedures, management controls, and managing the behavior of people" (p. 299). From the perspective of the employee, we use the term IS security environment to refer to one's perception of these technical, social, and organizational dimensions of IS security.

We briefly review three categories of IS security studies. The first category encompasses a large area of IS security research, which has focused on factors that determine one's compliance or non-compliance to IS security policies. Drawing on various theoretical perspectives (e.g., deterrence theory; protection motivation; neutralization), these studies have shown that perceptions of sanctions increase compliance or reduce violations to IS security policies (e.g., d'Arcy et al. 2009; Kankanhalli et al. 2003; Straub 1990). More recently, it has been suggested that deterrence may not be an ideal predictor of compliance behaviors, especially in the presence of other determinants such as moral factors or neutralizing cognitions (e.g. d'Arcy et al.'s 2009; Myyry et al. 2009; Siponen & Vance 2010). The second category of studies has sought to uncover different types of IS security behaviors. For example, Schultz (2002) developed a framework for understanding and predicting intentional and unintentional insider attacks. Similarly, Stanton et al. (2005) developed a taxonomy of security behaviors based on two underlying dimensions and their combinations: level of expertise and the intentionality of behavior. The third category shows that the IS security environment can also trigger negative consequences. For example, drawing on reactance theory, Lowry & Moody (2015) argued that IS security policies can undermine individual freedom and create an adverse state of arousal (i.e. reactance), which reduced compliance intentions.

We make several observations. First, all studies from the first and third categories looked at antecedents of compliance rather than the inner working of the compliance construct or its consequences. Studies from the second category address this issue partially by developing frameworks of non-compliant behavior. Second, compliance and non-compliance are considered as a uniform behavior or intention. However, non-compliance can comprise multiple dimensions of IS use (e.g., ineffective use; hindering creative use), some of which may extend beyond behavioral acts (e.g., emotional reactions such a frustration from the IS security environment; cognitive aspects; etc.). Third, most empirical results are based on scenario-based analysis (e.g., d'Arcy et al. 2009; Hu et al. 2011; Myyry et al. 2009; Siponen & Vance 2010). While this method has been well validated, it faces challenges with establishing ecological validity. This suggests a need to complement the extant research with studies in real-life settings where individuals have to face actual IS security issues and consequences that have a direct bearing on their work environment. Our study extends the existing literature by examining how individuals react to a stressful IS security environment. While non-compliance is one potential outcome that can occur (d'Arcy et al. 2014), stress research suggests there is likely to be a richer set of consequences including emotional, cognitive, and behavioral processes and their interactions. Addressing these issues is very important, given that the lack of fit between the characteristics of the environment and the individual can reduce compliance intentions (D'Arcy et al. 2014) and also lead to a set of other consequences such as reduced job satisfaction (Ragu-Nathan et al. 2008) and well-being (Cooper et al. 2001).

METHOD

As there is limited theoretical understanding on how individuals react to a stressful IS security environment, we used a qualitative and exploratory approach to investigate this issue. More precisely, we conducted a case study using an inductive approach based on semi-structured interviews with 41 participants. Case study research method has been used extensively in IS qualitative research (Darke, Shanks & Broadbent, 1998). For this research, the type of case study is exploratory as we are studying a situation that has no clear outcomes yet (Yin, 2003). This approach is particularly appropriate for this research project as conducting semi-structured interviews provides a rich understanding of security practices that are implemented in a hospital and their consequences on individuals.

Context

The healthcare setting for this case study was a two-hospital institution that uses multiple health information systems. The main system is an electronic health record system that handles the administrative and clinical aspects of care during a patient's stay at the hospital. Actors dealing with patient care (e.g., physicians; nurses; administrative staff) from admission to release of the patient have access to this system. They enter data at their level which is then immediately available to all authorized care providers through the electronic medical records.

Data Collection

In collaboration with the top management of the hospitals, we selected participants based on their job description and their use of the information systems in the hospitals. It was important to select participants with different functions and different levels of interactions with the systems, the patients, and the patients' health information. Participants were categorized in two main groups: medical and administrative (see Table 1 below).

Table 1. Participants of semi-structured interviews

Position	Number of Participants per Position
Medical position	
Doctor / Head of Unit	7
Doctor	10
Nurse	3
Administrative position	
Management	10
Administration	11
TOTAL	41

By medical participants, we mean those involved with patient care, such as doctors or nurses. By administrative participants, we mean those who are not involved with medical practice of patient care such as hospital managers, IT personnel, etc. On rare occasions, there was crossover between these areas, where a medical doctor was currently holding a fulltime administrative position. In that case, we took the point of view of their current position for the analyses.

Participants were interviewed for about 30 minutes using a semi-structured interview protocol. The interview protocol had three main groups of questions: how health information systems are used by participants; participants' perceptions about IS security; how they cope with their IS security environment. The qualitative data collection lasted two months.

PRELIMINARY RESULTS

A preliminary analysis of the interviews revealed some interesting results about the negative consequences of security practices and policies to care providers and patients.

Evoking negative emotions, which results in dissatisfaction with the system

One of the common practices that the hospital advised strongly to employees was to log off from the system after each usage. This practice had been in place to prevent undesired access to patients' information. However, this evoked strong negative emotions in care providers, which resulted in non-compliance behavior. The act of logging in and out was very frustrating for some of our participants. For example, a surgeon stated*: « Imagine you operate on ten patients, if you have to close your login session every time you do a surgery, and you come back you retype everything. At the end of the day, you will be sick of all of this." (P 13)*

Moreover, too much security made the usage of the system slow and difficult, which in some cases decreased care-providers' motivation to use the system. For example, one of the technical staff explained: *"Security is good but it should not become a big constraint because that's why things take longer… ah, there are many passwords, we need to remember* all our *passwords ... security is a constraint but it should not be too big a constraint, otherwise it penalizes the usage of products. That's for sure." (P.16)*. The negative feelings increased dissatisfaction with the system, which in turn triggered some levels of resistance towards it.

Ineffective usage of the system and putting patients' health at risk

To cope with the frustration due to too much security, some of the participants left their login sessions open, although they knew that this might increase security risks: This finding is in line with D'Arcy et al.'s (2014) observation that employees cope with the stress created from burdensome security policies by deliberately violating such policies. *It is not surprising that you leave your login session open. It is not due to negligence; it is because you say "after all, damn, I will not retype my password today for the twentieth time. It is their job to make sure it works properly."(P 13)*. Leaving login sessions open not only facilitates unauthorized access to patients' information, but can also yield mistakes such as through erroneous data entry by others. This will prevent traceability of information, which can be dangerous for patients. For example, an intern can add a prescription to a patient file in the name of a specialist. Since nurses or other physicians might not know the prescription was given by the intern, they might skip any further verifications to check for possible mistakes, which can put patients' health at risk.

Limiting creative usage of the system

Another observed negative consequence was that a stressful security environment was limiting creative usage of the system. Based on security chart of the hospital, it was not allowed that care-providers send patients' medical information to each other. However, some nurses and doctors developed a creative practice by which they would use their smartphones to communicate about the health status of patients. For example, nurses would send wound images, or medical test results directly to doctors using their smartphones. Doctors also sent them their diagnoses and advices through the same medium. This practice was considered unsafe by the hospital and was subsequently banned, which was perceived negatively by the care providers.

In sum, the preliminary analysis of some of our interviews showed that a stressful security environment in a health setting can result in emotional, cognitive, and behavioral processes like evoking negative emotions in users toward the system, increased dissatisfaction, limiting creative usage of IT, and increase of inappropriate workarounds, which can lead to ineffective usage of the system and eventually can put patients' health at risk.

CONCLUSION

As discussed earlier, the goal of this research-in-progress paper is to investigate how individuals react to a stressful IS security environment in a health care setting. While non-compliance (i.e. a behavioral consequence) is one potential outcome that has been observed in extant literature, our preliminary findings showed that there is likely to be a richer set of emotional, cognitive, and behavioral effects on care providers. By studying these effects and their interactions, we aim to create a better picture of the whole process and answer how people react to a stressful security environment and how that might influence care-providers, patients, and hospitals. This knowledge can eventually help us to design security control mechanisms which are not perceived stressful while providing adequate IS security.

Future steps of this project are to conduct more interviews and observations to code data primarily based on "emotional", "cognitive", and "behavioral" dimensions of IS security. Since the study is inductive in nature, we are open to finding new categories and codes along the way. Then, we will analyze our data and draw conclusions by category as we would like to see how these categories interact and if the medical group experiences the same challenges as the administrative group. We will form a process model to explain the processes that unfold, their interactions, and their long term effects.

REFERENCES

Appari, A. and Johnson, M.E., 2010. Information security and privacy in healthcare: current state of research. *International journal of Internet and enterprise management*, *6*(4), pp.279-314.

Cooper, C.L., Dewe, P.J. and O'Driscoll, M.P., 2001. *Organizational stress: A review and critique of theory, research, and applications*. Sage.

Darke, P., Shanks G., and Broadbent, M. 1998. “Successfully completing case study research: combining rigour, relevance and pragmatism”, Information Systems Journal, Vol. 8, pp. 273-289.

D'Arcy, J., Herath, T. and Shoss, M.K., 2014. Understanding employee responses to stressful information security requirements: a coping perspective. *Journal of Management Information Systems*, *31*(2), pp.285-318.

D'Arcy, J., Hovav, A. and Galletta, D., 2009. User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research*, *20*(1), pp.79-98.

Dhillon, G.,and Torkzadeh, G. 2006. Value-focused assessment of information system security in organizations. Information Systems Journal, 16(3), pp. 293-314.

Hu, Q., Xu, Z., Dinev, T. and Ling, H., 2011. Does deterrence work in reducing information security policy abuse by employees?. *Communications of the ACM*, *54*(6), pp.54-60.

Kankanhalli, A., Teo, H.H., Tan, B.C. and Wei, K.K., 2003. An integrative study of information systems security effectiveness. *International journal of information management*, *23*(2), pp.139-154.

Lowry, P.B. and Moody, G.D., 2015. Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. *Information Systems Journal*, *25*(5), pp.433-463.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T. and Vance, A., 2009. What levels of moral reasoning and values explain adherence to information security rules: an empirical study. *European Journal of Information Systems*, *18*(2), pp.126-139.

Ragu-Nathan, T.S., Tarafdar, M., Ragu-Nathan, B.S. and Tu, Q., 2008. The consequences of technostress for end users in organizations: Conceptual development and empirical validation. *Information Systems Research*, *19*(4), pp.417-433.

Schultz, E.E., 2002. A framework for understanding and predicting insider attacks. *Computers & Security*, *21*(6), pp.526-531.

Siponen, M. and Vance, A., 2010. Neutralization: new insights into the problem of employee information systems security policy violations. *MIS quarterly*, pp.487-502.

Stahl, B.C., Doherty, N.F. and Shaw, M., 2012. Information security policies in the UK healthcare sector: a critical evaluation. *Information Systems Journal*, *22*(1), pp.77-94.

Stanton, J.M., Stam, K.R., Mastrangelo, P. and Jolton, J., 2005. Analysis of end user security behaviors. *Computers & Security*, *24*(2), pp.124-133.

Straub Jr, D.W., 1990. Effective IS security: An empirical study. *Information Systems Research*, *1*(3), pp.255-276.

Yin, R.K. 2013. Case Study Research: Design and Methods, 5th Revised edition, SAGE Publications Inc.: Thousand Oaks.