Coping with Information Security Stressors in Healthcare

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

Shamel Addas
Queen’s University
shamel.addas@queensu.ca

Isabelle Fagnot
Audencia Business School
ifagnot@audencia.com

Abstract

Protecting the security of patients’ information is of tremendous importance to policy makers and healthcare researchers. Past research suggests that information security problems can be understood by using a stress/coping framework that examines information security stressors in the environment and the corresponding coping responses. Following this line of thinking, the present paper examines the following questions: What information security stressors are encountered in the healthcare environment? How do care providers cope with these stressors and what is the nature of the stress/coping relationship? To answer these questions, we conducted a case study based on semi-structured interviews with 41 health care providers in two hospital settings. Our findings show that the coping responses to information security stressors are not restricted to compliance/non-compliance behaviors. Stressors elicit an array of coping responses that cover a wide range of coping categories. Moreover, our results show a reciprocal relationship between stressors and coping responses.

Keywords

Information security, Healthcare, Stressors, Coping responses, Healthcare information technology

Introduction

Protecting the security of patients’ health information is a topic of tremendous importance to policy makers and healthcare information technology (HIT) researchers (Lowry and Moody 2015; Pouloudi et al. 2016; Siponen and Vance 2010). An estimated 120,000 security violations have occurred between 2003 and 2015 (Snell 2015) and the corresponding costs of legal settlements exceed $6 billion per year (Johnson and Willey 2011). Estimates indicate that 10% of health expenditures reimbursed by Medicare is paid to fraudulent providers and identity thieves (Appari and Johnson 2010). As these examples illustrate, information security issues in healthcare affect not only the patient side but also the providers (and their organizations) handling patient information.

Two dominant streams of research on information security in healthcare have examined this topic. The first stream focuses on privacy and security threats, such as understanding privacy concerns—and their antecedents and consequences—among healthcare patients (e.g., Anderson and Agarwal 2011; Sankar et al. 2003), or examining how and why internal and external agents access patient data inappropriately through abusing their privileges or exploiting vulnerabilities (Appari and Johnson 2010). The second stream examines solutions to privacy and security threats, such as implementing information security practices and the extent to which healthcare providers comply with such practices (e.g., Johnston and Warkentin 2008; Warkentin et al. 2006).
Coping with information security stressors

Taken together, these two streams can be viewed as focusing on two sides of the same phenomenon, with one concentrating on the underlying information security threats and the other on the appropriate responses to such threats. The persons experiencing the threats and responding to them can be the same entity (e.g., a patient or a provider) or different entities (e.g., a provider implementing a security solution to protect patients from information security threats). In line with this viewpoint, several researchers suggest that information security problems can be understood by using a stress/coping framework that considers security threats and challenges as stressors in the environment and examines how people respond by implementing different coping responses (D’Arcy et al. 2014; Herath et al. 2014; Johnston and Warkentin 2010; Liang and Xue 2009).

Applying this lens to extant research on information security in healthcare, we identify three gaps in our understanding of security-related stressors and coping responses. First, the coping responses studied are mostly restricted to compliance/non-compliance behaviors. For example, several researchers examine compliance-related outcomes such as the willingness to disclose or provide access to information (Anderson and Agarwal 2011; Sankar et al. 2003) and the intentions to comply (Johnston and Warkentin 2008) or the actual compliance to privacy and security regulations (Kwon and Johnson 2013). Others focus on the non-compliance side and investigate issues such as the likelihood of healthcare security rule violation (Wall et al. 2016). While these studies have advanced our understanding of the factors that promote or inhibit compliance and non-compliance, we still have a limited understanding of other potential and qualitatively different coping responses. For example, coping literature indicates that compliance and non-compliance responses cover but two possible categories (accommodation and opposition) from within a much larger list of coping categories (Skinner et al. 2003).

Second, research tends to consider that a given privacy or security stressor in the environment (i.e., a threat or challenge) will elicit a single coping response or a uniform coping pattern (i.e., a number of coping responses from within the same coping category). For example, some studies examine the effect of privacy/security threat appraisal on an individual’s willingness to provide access to personal health information (Anderson and Agarwal 2011). Others have looked at the impact of privacy concerns on accommodating behaviors such as seeking medical care and/or on information disclosure once care is sought (see Sankar et al. 2003 for a review). What these studies overlook is that a given environmental stimulus can often elicit an array of different or mixed emotional and behavioral responses (Beaudry and Pinsonneault 2010; Stein et al. 2015). This can be especially true in the context of healthcare information security, which—given the nature and variety of the risks involved—can trigger a set of intense and emotionally charged reactions (Anderson and Agarwal 2011).

Finally, extant healthcare IT research considers stressors and coping responses in a linear and somewhat disjointed fashion. However, this relationship is likely to be more complex. For example, coping responses can alter the actual terms of the person-environment relationship, in some cases potentially becoming a renewed source of stress (Folkman and Lazarus 1988). While this notion of a reciprocal relationship between stress and coping has been long recognized in the coping literature (e.g., Aldwin and Stokols 1988), it still awaits empirical testing.

This paper addresses these gaps in research by developing a comprehensive account of stressors (i.e., events that are appraised negatively as threats or positively as challenges) and coping responses relating to HIT and particularly information security aspects. We address two research questions: What information security stressors are encountered in the healthcare environment? How do care providers cope with these stressors and what is the nature of the stress/coping relationship? We focus on stressors and coping responses for providers who are handling patients’ health information. Drawing on Skinner et al.’s (2003) coping taxonomy, we identify a range of stressors and their corresponding coping responses that are used by healthcare professionals in two leading hospital institutions in France. We show that a given stressor can elicit an array of coping responses and that these responses or strategies cover a wide range of coping categories. Our focus on stress/coping episodes also allows us to unearth the complex relationship between stressors and coping responses. Our findings contribute to extant research on healthcare information security and to the wider literature on information security. Specifically, our findings advance our understanding of how individuals experience different information security stressors in their work environment and the range of coping responses they implement (including a mix of emotional and behavioral responses). As well, our results extend research by empirically showing that there is a reciprocal relationship between stressors and coping responses over time.
In the next section, we describe the main elements of coping theory that are relevant for our study. We then present the context of our qualitative study and describe what data we collected and how the data were collected and analyzed. After that, we present the results by focusing on the key coping episodes we found and the stressors and coping responses contained within these episodes. This is followed by a discussion of our findings and their implications for research and practice. We end the paper by offering concluding thoughts.

**Theoretical Background: Coping Theory**

Coping can be defined as a person's cognitive and behavioral efforts to manage stressful situations (Folkman and Lazarus 1988). Stress arises when the environmental demands are appraised by the person as exceeding his or her abilities and resources (Folkman et al. 1986; Lazarus 1993). During the appraisal process the person evaluates whether there is potential harm or benefit in the situation, and then if anything can be done to prevent harm or to improve the prospects for benefit (Folkman et al. 1986). That is, the object of coping (stressor) is seen as a challenge (i.e., having the possibility of mastery and benefit) or threat (i.e., having the possibility of harm or loss) (Lazarus and Folkman 1984). In coping theories, there is also an emphasis on the context-dependent nature of coping. Thus, coping is influenced both by the person's appraisal of the stressful situations and the resources available for managing them (Folkman et al. 1986).

Coping responses or strategies are actions that individuals take to respond to stressful situations (Skinner et al. 2003). For example, people might avoid the situation, adopt problem-solving strategies, or seek help, among others. These actions can include both behavioral and cognitive responses. Coping responses are used to resolve the stressor and improve one's mental and physical well-being (Skinner et al. 2003). If coping responses are constructive, they can lead to coping resources such as self-reliance and confidence. On the other hand, using unconstructive responses can lead to low self-efficacy and the accumulation of vulnerabilities. However, there is no inherently good or bad coping response (Folkman et al. 1986).

Coping responses have been categorized differently in the extant literature. Folkman and Lazarus (1980) used a functional approach that categorized them as problem- vs. emotion-focused coping, which basically highlights rational versus emotional reactions to stressful events. Problem-solving coping aims at managing the problem that causes distress. On the other hand, emotion-focused coping aims at regulating the emotional responses to the problem (Lazarus and Folkman 1984). However, this functional categorization has been criticized for not being exhaustive (e.g., seeking social support cannot be clearly categorized under either category) and not having mutually exclusive categories (i.e., observed coping responses can serve both functions and thus fit into both categories) (Skinner et al. 2003).

Approach and avoidance is another way of distinguishing coping responses based on the nature of one's orientation toward the stressful stimuli (Roth and Cohen 1986). Approach brings an individual to a closer contact with the stressful situation and this provides opportunity for instrumental action. In contrast, avoidance allows an individual to withdraw attention from the stressful stimuli, which may alleviate the distressing experience and provide safety (Roth and Cohen 1986). This classification has also been criticized for not having clearly defined categories and because coping responses are multidimensional and many responses cannot be clearly assigned to either category (e.g., seeking social support; information seeking) (Skinner et al. 2003).

To address these limitations, Skinner et al. (2003) propose a hierarchical taxonomy of coping (see Table 1). This taxonomy is based on 12 types of coping responses (also called families of coping) that are classified into three sets of general adaptive processes, each containing four coping responses. The three adaptive processes are directed toward the environment (to achieve control), the self (to achieve autonomy), or other people (to achieve relatedness). Within each set, there are two coping responses for which the stressful situation is appraised as a challenge and two responses where the situation is appraised as a threat. Each coping response (e.g., problem solving) can be further decomposed into different ways of coping (e.g., strategizing; instrumental action; planning). Ways of coping refer to the ways people actually respond to stress (Skinner et al. 2003). Because Skinner et al.’s (2003) taxonomy addresses many of the classification problems encountered in the literature and given its wide popularity, we adopt the taxonomy as a way to understand the coping responses used by care providers in response to healthcare IT stressors.
Table 1. Coping Responses (adapted from Skinner et al. 2003)

<table>
<thead>
<tr>
<th>Adaptive process</th>
<th>Coping responses (triggering appraisal)</th>
<th>Description (ways of coping)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coordinate actions with contingencies in the environment (directed toward environment to achieve control)</td>
<td>Problem solving (challenge appraisal)</td>
<td>Adjust actions to be effective (strategizing; instrumental action; planning)</td>
</tr>
<tr>
<td></td>
<td>Information seeking (challenge appraisal)</td>
<td>Find additional contingencies (reading; observation; asking others)</td>
</tr>
<tr>
<td></td>
<td>Helplessness (threat appraisal)</td>
<td>Find limits of actions (confusion; cognitive interference; cognitive exhaustion; freezing)</td>
</tr>
<tr>
<td></td>
<td>Escape (threat appraisal)</td>
<td>Escape noncontingent environment (behavioral avoidance; mental withdrawal; denial; wishful thinking)</td>
</tr>
<tr>
<td>Coordinate reliance with social resources available (directed toward others to achieve relatedness)</td>
<td>Self-reliance (challenge appraisal)</td>
<td>Protect available social resources (emotion regulation; behavior regulation; emotional expression; emotion approach)</td>
</tr>
<tr>
<td></td>
<td>Support seeking (challenge appraisal)</td>
<td>Use available social resources (contact seeking; comfort seeking; instrumental aid; social referencing)</td>
</tr>
<tr>
<td></td>
<td>Delegation (threat appraisal)</td>
<td>Find limits of resources (maladaptive help seeking; complaining; whining; self-pity)</td>
</tr>
<tr>
<td></td>
<td>Social isolation (threat appraisal)</td>
<td>Withdraw from unsupportive context (social withdrawal; concealment; avoiding others)</td>
</tr>
<tr>
<td>Coordinate preferences with available options (directed toward self to achieve autonomy)</td>
<td>Accommodation (challenge appraisal)</td>
<td>Flexibly adjust preferences to options or constraints (distraction; cognitive restructuring; minimization; acceptance)</td>
</tr>
<tr>
<td></td>
<td>Negotiation (challenge appraisal)</td>
<td>Find new options (bargaining; persuasion; priority setting)</td>
</tr>
<tr>
<td></td>
<td>Submission (threat appraisal)</td>
<td>Give up preferences (rumination; rigid perseveration; intrusive thoughts)</td>
</tr>
<tr>
<td></td>
<td>Opposition (threat appraisal)</td>
<td>Remove constraints (other-blame; projection; aggression)</td>
</tr>
</tbody>
</table>

Research Methodology

As there is limited theoretical understanding on how individuals cope with information security stressors, we used a qualitative and exploratory approach to investigate this issue. We conducted a case study using an inductive approach based on semi-structured interviews with 41 participants. The case study research method has been used extensively in IS qualitative research (Darke et al. 1998). Since we are studying a phenomenon that has no clearly established outcomes, our case study is exploratory in nature (Yin 2003).

Context

The healthcare setting for this case study is a two-hospital institution. The two hospitals are private non-profit university hospitals and part of the same medical group. The hospitals use 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 that then becomes immediately available to all authorized care
providers through the electronic medical records. Our choice of setting follows a purposeful sampling strategy. Because our goal was not to generalize to broad hospital populations, we did not seek a large representative sample. Rather, we opted for intensity sampling, where our choice of two information-rich cases allowed our phenomenon of interest to be manifested clearly (Patton 2005).

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 into two main groups: medical and administrative (see Table 2 below).

<table>
<thead>
<tr>
<th>Position</th>
<th>Number of Participants per Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medical position</td>
<td></td>
</tr>
<tr>
<td>Doctor / Head of Unit</td>
<td>7</td>
</tr>
<tr>
<td>Doctor</td>
<td>10</td>
</tr>
<tr>
<td>Nurse</td>
<td>3</td>
</tr>
<tr>
<td>Administrative position</td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td>10</td>
</tr>
<tr>
<td>Administration</td>
<td>11</td>
</tr>
<tr>
<td>TOTAL</td>
<td>41</td>
</tr>
</tbody>
</table>

Table 2. Participants of Semi-structured Interviews

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 information security stressors, and how they cope with these stressors. The qualitative data collection lasted two months and the interviews were recorded and then transcribed for analysis.

Data Analysis

In the first phase of the analysis, a coding scheme was developed based on Skinner et al.’s (2003) categorization of coping responses. Accordingly, the interview transcripts were coded into the corresponding coping response categories [COPING RESPONSE]. The transcripts were also coded by type of environmental stressor [STRESSOR], the person facing and appraising a stressor [PERSON], the conditions existing in the environment that trigger the stressor [INITIAL CONDITION], and the outcomes of coping [OUTCOME]. NVivo v.10 was used to facilitate the coding process. Coding was done by all the authors. Moreover, the authors compared their coding after having coded three interviews to calibrate the coding process.

In the second phase of the analysis, one or multiple coping episodes were constructed based on each interview. Each coping episode describes a situation in which a healthcare provider (e.g., a doctor or a nurse) faces a stressor and he or she responds to that stressor. Further, if the coping outcome was stated or implied, it would be described in the episode. Below is an example of a coping episode constructed based on interview 13:

“An orthopedic surgeon [PERSON] uses different medical software for doing his job and for each software he needs to enter a unique password. Being forced to enter many passwords and also his demanding nature of work put a lot of pressure on him and create a stressful situation [STRESSOR]. To respond to this stressful situation, he intentionally leaves his computer sessions open to be able to use them later on without the need to log in again and
reenter his passwords. This act basically is against hospital rules that asks employees to close the sessions after each usage [COPING RESPONSE- OPPOSITION]. This creates a possibility that someone who is not authorized have access to patients’ data [OUTCOME].”

Finally, the data were analyzed by comparing and contrasting coping episodes.

**Results**

Figure 1 explains the appraisal process of information security stressors and its possible consequences. As shown in Figure 1, initial conditions such as technical issues, behavioral issues, or hospital regulations can trigger a stressful situation (i.e., security stressor) for healthcare providers (i.e., nurses, doctors, managers, or general staff). For example, hospital regulations require surgeons to use multiple passwords for their systems. This can create stress in surgeons since they have a demanding work environment and they usually work under pressure. After facing the stressful situation, the healthcare provider evaluates the situation and can appraise it as a challenge or threat. In the next step, he or she reacts by using one or multiple coping responses (coping responses 1 to n refer to those responses identified by Skinner et al. 2003). For example, the surgeon might leave his or her login sessions open and complain about the situation to other colleagues (i.e., multiple coping responses). Consequently, the reactions to the stressful situation can create an outcome that in turn can trigger a new stressful situation. Following the same example, leaving the sessions open can results in unauthorized access to the surgeon’s data, which can become a new source of stress for the surgeon.

Our analysis yielded three findings: 1- the identification of information security stressors and their coping responses in a healthcare setting, 2- the possibility of having more than one coping responses for each stressor, and 3- the interrelation of stressors and coping responses (i.e., chains of stressors). These findings are discussed below.

**Figure 1. Coping Model of Information Security Stressors in Healthcare**

**Identification of Information Security Stressors and their Coping Responses**

As shown in Figure 1, we identified the unauthorized access to data as a main source of information security-related stressors in healthcare. Further, we found out that the initial conditions that created such stressors were mostly related to: 1- Technical issues, 2- Behavioral issues (IT misuse), and 3- Hospital regulations. Unauthorized access to data happened when someone intentionally or unintentionally accessed patients’ data although he or she was not allowed to. This stressor was mostly due to misuse of the system (e.g., using someone else’s password) or/and hospital’s security regulations (e.g., requiring
staff to have a unique password for each software and to change it frequently can make them leave their sessions open. For instance, one participant mentioned “A colleague got sick (was hospitalized here) and some colleagues looked at his medical record (...). The colleague who was sick found out. Then top management sent a reminder that this is not allowed.” (i.e., misuse of the system) (Interview 30).

We observed that healthcare providers (i.e., doctors, nurses, managers, or general staff) evaluated the information security stressors (i.e., appraisal) and coped with them using different strategies or responses. It is important to note that coping responses to security stressors were not restricted to compliance or non-compliance. Healthcare providers used constructive responses such as problem solving, information seeking, support seeking, accommodation, and negotiation. Moreover, unconstructive coping responses such as helplessness, escape, submission, and opposition were used as well. For example, a nurse thought that in general IT could not be trusted because all the information was shared and anyone who had the knowledge could always find a way to steal information without being traced. This perception created a stressful situation for her (security stressor). However, she was not capable of changing the situation and felt very helpless (coping response-helplessness).

**Multiple Coping Responses for each Stressor**

Our data showed that healthcare providers might use one or multiple coping responses to an information security stressor (see Table 3). For example, a head nurse was concerned that computer screens displaying patient information were easily visible to people who passed by in the corridors. She further explained that computers took a long time to shut down the system (i.e., a technical issue) and this created the possibility of impermissible disclosures. She believed that if everything were on paper, they would not have had such problems and she wished everything were like before (coping response- Helplessness). Moreover, she did not do anything to solve the problem (coping response- escape).

<table>
<thead>
<tr>
<th>Stressor</th>
<th>Examples</th>
<th>Coping response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized access to data</td>
<td>The system is slow and shuts down very late; therefore, monitors can be seen by everyone in the corridors [technical issue]</td>
<td>Not providing any solution and just wishing everything was like before with paper medical records (helplessness)</td>
</tr>
<tr>
<td></td>
<td>Nurses looking up the health information of people they know [misuse]</td>
<td>Talking to nurses to change their behavior (negotiation)</td>
</tr>
<tr>
<td></td>
<td>Having too many passwords to manage [misuse, hospital regulations]</td>
<td>Leaving their session open when it is possible so that they do not have to retype passwords (opposition)</td>
</tr>
<tr>
<td></td>
<td>Stealing someone’s password and accessing patients’ information [misuse]</td>
<td>Complaining about the situation and blaming others (opposition)</td>
</tr>
<tr>
<td></td>
<td>Sending images of patients’ wounds by smartphones to doctors [misuse]</td>
<td>Talking to nurses or doctors who do that to change their behavior (negotiation)</td>
</tr>
<tr>
<td></td>
<td>Interns change frequently and they have access to all patients’ data [misuse, hospital regulations]</td>
<td>Complaining about the situation and blaming others (opposition)</td>
</tr>
</tbody>
</table>
Younger medical staff use their personal smartphones all the time to communicate and access medical information on Vidal online

| Head of unit decided to allow controlled access to personal smartphones and to communicate with them via text messaging rather than email which they don’t read (negotiation) |

Table 3. Examples of Information Security Stressors and their Coping Responses

Chains of Stressors

Our data revealed that responses to non-security or security stressors might initiate a new security stressor. As shown in Figure 1, there can be a feedback loop between the outcome and the stressor. That is, the outcome of coping responses might give rise to a new stressor in the organization. For example, surgeons needed to work with multiple software and they needed to log in and out of them frequently, while for each software they had to enter a unique password. This situation on top of their demanding work was very stressful (i.e., non-security stressor). To cope with the stressor, the surgeons left their computer sessions open (i.e., opposition). Consequently, anyone passing by could potentially access the system and data (i.e., a new security stressor: unauthorized access to data), which defeated the purpose of using passwords to protect patient data and triggered the emotion of fear.

As another example, a head nurse reported that other nurses were sometimes tempted to access information on patients they were not caring for (e.g., someone they knew) (i.e., security stressor for the head nurse). To cope with the stressor and resolve the problem of unwanted data access, the head nurse discussed the issue with the vendor and the vendor came up with a proposal to limit the nurses’ access to the patients’ data within the unit to which the nurses are assigned (i.e., problem solving). This became a new source of stress to the head nurse, because it meant that nurses with transversal roles who were assigned flexibly to multiple units would have to work less flexibly or risk losing access to relevant data (non-security stressor). Consequently, this stressor gave rise to two simultaneous coping responses: rejecting the vendor’s solution and refusing to implement that functionality (i.e., opposition) and continuing to work with the vendor to find a better solution (i.e., negotiation).

Discussion and Conclusion

The contributions of this research are threefold. First, the extant literature on healthcare information security has often discussed compliance and non-compliance as the main coping responses (e.g., Anderson and Agarwal 2011; Johnston and Warkentin 2008; Kwon and Johnson 2013; Wall et al. 2016), with other coping responses remaining largely uninvestigated. Perhaps due in part to the nature of healthcare IT, the sensitive nature of patients’ information, and the emotional aspects of the care delivery process, the present study observed coping responses such as problem solving, opposition, submission, escape, help seeking, and accommodation that have been overlooked in past IS research.

Second, we observed that a person might use one or multiple coping responses to a security stressor. Extant research tends to consider that a given security stressor in the environment will be appraised either as a threat or challenge, which consequently will elicit only a single coping response or a uniform coping pattern (Anderson and Agarwal 2011). However, a given stimulus can often elicit an array of different or mixed emotional and behavioral responses (Beaudry and Pinsonneault 2010; Stein et al. 2015). Our observation shows that health care providers often appraised a security stressor as both threat and challenge, and therefore responded using both constructive and unconstructive responses.

Third, our results extend research by empirically showing that there is a reciprocal relationship between stressors and coping responses over time. That is, responses to non-security or security stressors might initiate a new security stressor.

These findings have practical implications. Interview data shed light on how some hospital regulations that were put in place to enhance the information security environment have had a different impact than intended depending on the coping responses that can greatly vary in any given situation.
Our study suggests directions for future research. Data on coping responses suggest that coping mechanisms may vary based on the position of the participant in the organization. That is, processes or stressors can be different due to roles and data handling responsibilities of healthcare providers. This needs further investigation.

REFERENCES


Coping with information security stressors


