UNDERSTANDING SECURITY AWARENESS IMPACTS ON HEALTHCARE TECHNOLOGY AVOIDANCE BEHAVIOR

Bahae Samhan, Illinois State University, College of Business, Department of Accounting and Business Information Systems, Normal, IL, 208-596-0195, bmsamha@ilstu.edu

ABSTRACT

This study empirically tests the impact of information security awareness on mitigating healthcare providers' technology avoidance behavior towards electronic health records. It provides a model that integrates concepts from the Information Security Policy Compliance Theory (ISPCT) and the Technology Threats Avoidance Theory in the context of healthcare. The study provides insights about the effect of information security awareness on healthcare providers' behavior towards healthcare technology. The findings reveal that technology avoidance can be predicted by levels of perceived threat, avoidance motivation, and information security awareness. The study also controlled for a few variables and found that age had significant influence on healthcare providers' avoidance behavior towards the healthcare technology.

Keywords: Electronic Medical Records (EMR), Healthcare Information Technology (HIT), Information Security Awareness, Information Security Policy Compliance Theory (ISPCT), Technology Avoidance, Technology Threat Avoidance Theory (TTAT).

INTRODUCTION

The implementation of Healthcare Information Technology (HIT) within healthcare organizations such as hospitals, clinics, and private practices are constantly increasing. In the United States, the government is providing incentives to healthcare organizations that are adopting specialized HIT such as Electronic Medical Records (EMR) (CMS report, 2017) to encourage a fully electronic healthcare system in the country.

Despite the potential benefits HIT can provide to healthcare organizations, healthcare providers tend to avoid using these technologies (Samhan and Joshi, 2017). This is particularly true for EMR because healthcare providers usually perceive it as a burden that hurdles them from performing their job of providing care to patients (Samhan, 2016). Healthcare providers may perceive EMR requirements to be unnecessary and consider it as additional tasks that may affect their professional status (Lapointe and Rivard, 2005). Healthcare providers have also expressed concerns about EMR affecting the way they communicate with patients while diagnosing them such as the loss of eye contact (Cotea, 2010). Additionally, it was found that healthcare providers consider EMR to be time consuming and working with it takes away valuable time from caring for patient, which makes the art of their job impersonal (Sassen, 2009).

In a recent study, Samhan and Joshi (2017) found that one of the main predictors of technology avoidance was perceived threat. They found that 73% of healthcare providers' responses about perceived threat considered cyber-security issues as a main concern. Cyber-security is an important topic in healthcare. The KPMG Healthcare Cybersecurity Survey of 2015 shows that more than 80% of healthcare executives reported that their healthcare organization was a victim of at least one cyber-attack in the past 2 years. Additionally, 13% of them reported being a victim of an external hacking attempt, some reported having such attacks on daily basis.

These attacks not only affect the security and privacy of healthcare data, but also may cause sever monetary damages to the organization. According to the fifth annual benchmark study on privacy and security of healthcare data of 2015, in the past two years, 90% of healthcare organizations had a data breach and 40% of which had at least five security breach incidents, which resulted in a $6 billion loss to the healthcare industry.

Healthcare organizations, that are becoming more digitalized, are becoming aware of cyber risks and thus are taking certain measures to raise their employees' awareness about cyber-security related issues. This includes making them more aware of the security and privacy policies of the healthcare organization (Bulgurcu et al., 2010), providing them with educational material about cyber-security (Locasto et al., 2011), and increasing the IT security mechanism of the healthcare organization such as the use of powerful anti-spyware software or firewall protection (Lee and Kozar, 2008).

However, we still find a dearth of research on user security behavior (Liang and Xue, 2010), especially in healthcare settings (Samhan, 2017). Further, majority of research on data security focused on the organizational level (D'Arcy et al., 2009; Straub and Welke, 1998) and limited research considered studying security behavior on the individual level (Liang and Xue, 2010). More importantly, there are limited studies that evaluates the impact of cyber security awareness on levels of technology adoption, resistance, and avoidance.

This study aims to investigate on an individual level how healthcare providers react when facing IT threats, and how does their security awareness levels play role in mitigating their technology avoidance decisions. To do so, this study empirically tests an integrative model that bridges concepts from the Technology Threat Avoidance Theory (TTAT) (Liang and Xue, 2010) with concepts of the Information Security Policy Compliance Theory (ISPCT) (Bulgurcu et al., 2010).

THEORETICAL BACKGROUND

TTAT was developed by analyzing the research conducted within areas of healthcare, psychology, risk analysis, and information systems. Technology threat avoidance is defined as the cybernetic process where users plan to enhance the difference between the current safe state and the unsafe end state resulting from using the technology (Carver and Scheier, 1982; Edwards, 1992; Carver, 2006; Liang and Xue, 2009).

The TTAT explains the main predictors influencing technology avoidance motivations in terms of three main stages. First, the threat appraisal stage, which suggests that users who perceive risks associated with the use of the technology will consider the technology as a threat. Second, the coping appraisal stage, and within this stage users begin to look for appropriate safeguarding measures that will help them avoid the perceived threats. Third, the coping stage, and here users begin to apply the chosen safeguarding measure to avoid the threat associated with the technology (Liang and Xue, 2009).

TTAT suggests that users, who perceive threats associated with the technology and those who find an available safeguarding measure that could be applied to minimize threats, will be more likely to avoid interacting with the technology. Therefore, the TTAT posits that perceived threat and safeguard availability have direct influence on avoidance motivation.

This study integrates the TTAT concepts with concepts of information security awareness from the ISPCT. According to ISPCT, the Information Security Awareness (ISA) is a second order construct that is shaped by the General Information Security Awareness (GISA) construct and the Information Security Policy Awareness (ISPA) construct.

GISA refers to users' overall knowledge and understanding of information security issues and its consequences (Bulgurcu et al., 2010). This includes users' overall knowledge about information security topics, which could be stemming from the exposure to external resources of security information, such as information security documents, information security workshops, news, or professional journals. It can also be obtained from having previous experiences with information security situations such as beaning a victim of a cyberattack.

ISPA refers to users' awareness of the rules and regulations of the policy in place (Bulgurcu et al., 2010). This includes users' knowledge and understanding of the security requirements prescribed by the organization and the aims of those requirements. Organizations may have specific expectations of users, which are reflected in security policies. Therefore, ISPA is a sense of awareness and commitment to the security objectives of these requirements and expectations. It is different from GISA. For example, a user may have general awareness of protecting digital information when using a username and password to login, yet he/she may not be aware that according to the information security policy at the organization, employees are required to change the password every few months, or that passwords must be of a certain length (Bulgurcu et al., 2010).

RESEARCH MODEL AND HYPOTHESIS

This study examines the impact of information security awareness on technology avoidance in a healthcare setting. Information security awareness is conceptualized based on the findings of the ISPCT, which suggests that information security awareness is a second order construct that is formed based on two main constructs: general information security awareness and information security policy awareness. On the other hand, avoidance is conceptualized based on the TTAT, which explains avoidance behavior from a threat perspective. It suggests that once a threat is perceived users would evaluate safeguarding measures to be taken in an aim to avoid the threat associated with the use of the technology.

Avoidance motivation refers to the degree to which healthcare providers are motivated to avoid the EMR by taking safeguarding measures (Liang and Xue, 2010). Generally, human tend to avoid losses in all aspects of their lives as much as possible (Freud, 1915; James, 1890). Therefore, when healthcare providers associate IT threats such as privacy invasion, potential loss of data, or financial losses with their use of the EMR, they become motivated to avoid it. This may be further explained by Maslow's hierarchy of needs, which suggests that securing resources and properties is a basic human need (Maslow, 1943). The positive relationship between perceived threat and avoidance motivation has been confirmed by numerous studies (Liang and Xue, 2010; Arachchilage and Love, 2014; Xue and Liang, 2014). Thus, this study hypothesizes that as EMR threat perception increases, healthcare providers become more motivated to avoid using it.

H1: Perceived threat positively affects avoidance motivation.

Healthcare providers' avoidance motivation may be affected by their awareness of the existing information security measures. There are many factors that can influence motivations of a given behavior (Ajzen and Albarracin, 2007). Fishbein (2008) suggests that any behavior can have endless number of variables predicting its motivations. Additionally, the Theory of Planned Behavior (TPB) (Ajzen, 1991) shows the possibility of having a non-TPB construct predicting an

effect on any of the TPB constructs including intentions, which in this study is equivalent to motivations (Ajzen and Albarracin, 2007; Fishbein, 2008; Conner and Armitage, 1998).
The influence of information security awareness on healthcare providers' avoidance motivation can be explained using the work of the innovation decision process to information security [27] by viewing information security awareness as knowledge, avoidance motivation as persuasion, and avoidance behavior as a decision. Healthcare providers' information security awareness can help shape levels of avoidance motivation to describe persuasion. According to [27], the persuasion stage can affect decisions, which means in the context of this study that avoidance motivation can affect healthcare providers' decision to avoid the EMR. This is consistent with prior research suggesting that security awareness is the most important factor in persuading individuals to change their actions [6, 32]. Therefore, it is hypothesized that:

H2: Information security awareness negatively affects avoidance motivation.

Safeguard availability refers to healthcare providers' capability to adopt a safeguarding measure that can be effectively applied to avoid the perceived threat (Liang and Xue, 2009). According to the TTAT, after a threat is perceived, healthcare providers will begin the coping appraisal process to evaluate potential safeguarding measures (Liang and Xue, 2010). The more healthcare providers perceive the safeguarding measure to be an available safeguard is perceived as effective, the more healthcare providers perceive the safeguarding measures as available the more the will be motivated to use it in order to avoid interacting with the EMR. This is similar to the concept of the response efficacy in protection motivation theory (Rogers, 1975; Rogers, 1983), and the concept of perceived benefits in the health belief model (Janz and Becker, 1984; Rosenstock, 1974); both of which were found to predict behavior likelihood or motivation. Prior research on information security have suggested that the availability of a safeguarding measure can motivate users to perform security behaviors (Anderson and Agarwal, 2006; Ng et al., 2009; Woon et al., 2005), which in this study would be avoiding the EMR.

H3: Safeguard availability positively affects avoidance motivation.

Following the framework of the TTAT, this study does not differentiate between motivation and intention. Fundamentally, avoidance motivation can be manifested by the behavioral intention to use the safeguard (Liang and Xue, 2010). Prior behavioral research such as (Ajzen, 1991; Ajzen and Fishbein, 1980; Fishbein and Ajzen, 1975) suggest that intention is a strong predictor of the studied behavior. This relationship has been confirmed by many IT adoption studies (e.g., Venkatesh et al., 2003). Therefore, it is theorized that avoidance behavior can be predicted by levels of users' motivation (intentions) to avoid the technology.

H4: Avoidance motivation positively affects the EMR avoidance behavior.

In addition to the main constructs of the integrated model, this study controlled for a number of variables, these are: Age, gender, and levels of technical skills. Additionally, it is argued that healthcare providers with different positions at the hospital would perceive different threats and would tolerate risk differently. Thus, we included position at hospital as a control variable. Figure 1 illustrates the research model of this study.

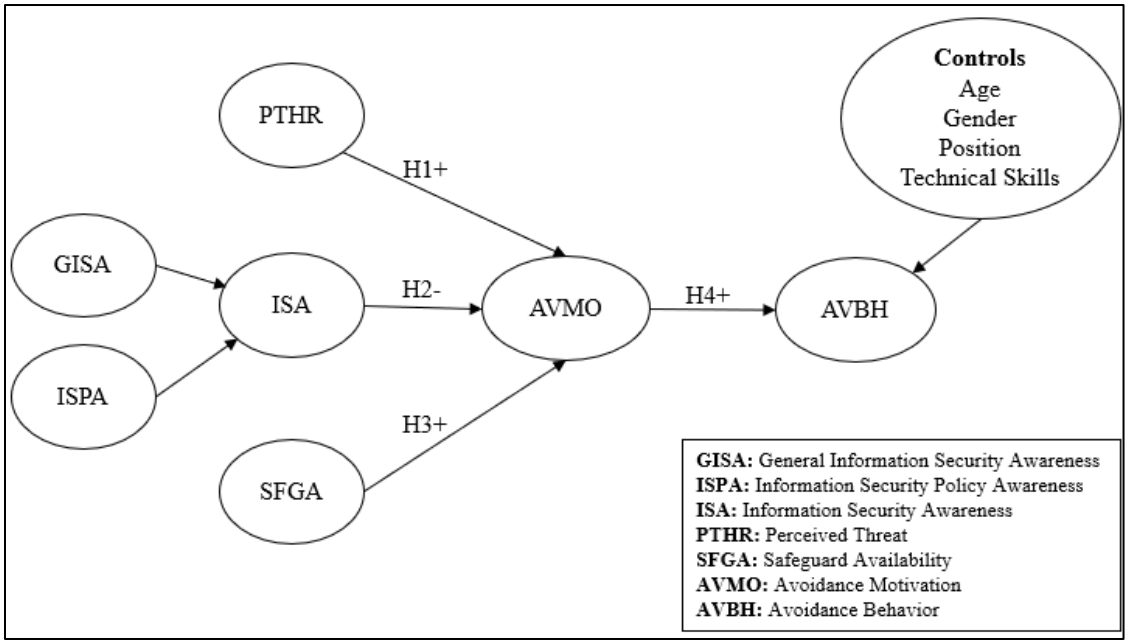

Fig. 1: The Research Model

METHODOLOGY

Instrument Development

Existing validated scales were adopted for this study. The survey items used for the model were mainly derived from the TTAT and the ISPCT. However, all items were modified to fit the context of the study. Measurement items were anchored on five-point Likert scales (1 = strongly disagree, 5 = strongly agree). The instrument was reviewed by IS researchers before collecting data.

Sample and Data Collection

Data were collected from healthcare providers from three different hospitals located in the Midwest states. Survey was sent electronically to 1,224 employees. The total valid collected responses were 237.

Instrument Validation

To validate the survey instrument, the psychometric properties of the survey were assessed by conducting Explanatory Factor Analysis (EFA) and Confirmatory Factor Analysis (CFA). Cronbach's α was performed to test for items reliability. After collecting data, CFA analysis was conducted and all items were found to have a significant loading greater than (0.7). All constructs had Cronbach's α values exceeding (0.8). The CFA analysis provided strong support for our measurement model, which suggested that the items under each of the constructs were adequately measuring the constructs.

The survey responses came in waves: (W1: N=117; W2: N=120). I checked for nonresponse bias by testing the difference in means between waves, and no significant differences were found between the two respondent groups based on the sample attributes (gender, age, and position).

RESULTS

The research model was evaluated using Structural Equation Modeling (SEM). The maximum likelihood estimator with robust standard errors (MLR) was applied. Because the model is not saturated (i.e., not all possible regression paths were included) the model fit indicators was evaluated.

All hypotheses were confirmed. Perceived threat had a significant positive effect on avoidance motivation ($b = .29$, $p < .01$), safeguard availability had a significant positive effect on avoidance motivation ($b = .31$, $p < .01$), the second order construct information security had a significant negative effect on avoidance motivation ($b = -.18$, $p < .01$), and avoidance motivation had a significant positive effect on the avoidance behavior ($b = .14$, $p < 0.01$).

The model accounts for 64% of variance in avoidance motivation and 49% of variance in avoidance behavior. Age and technical skills had positive direct effect of avoidance behavior. Figure 2 shows the results of the SEM analysis of the proposed model.

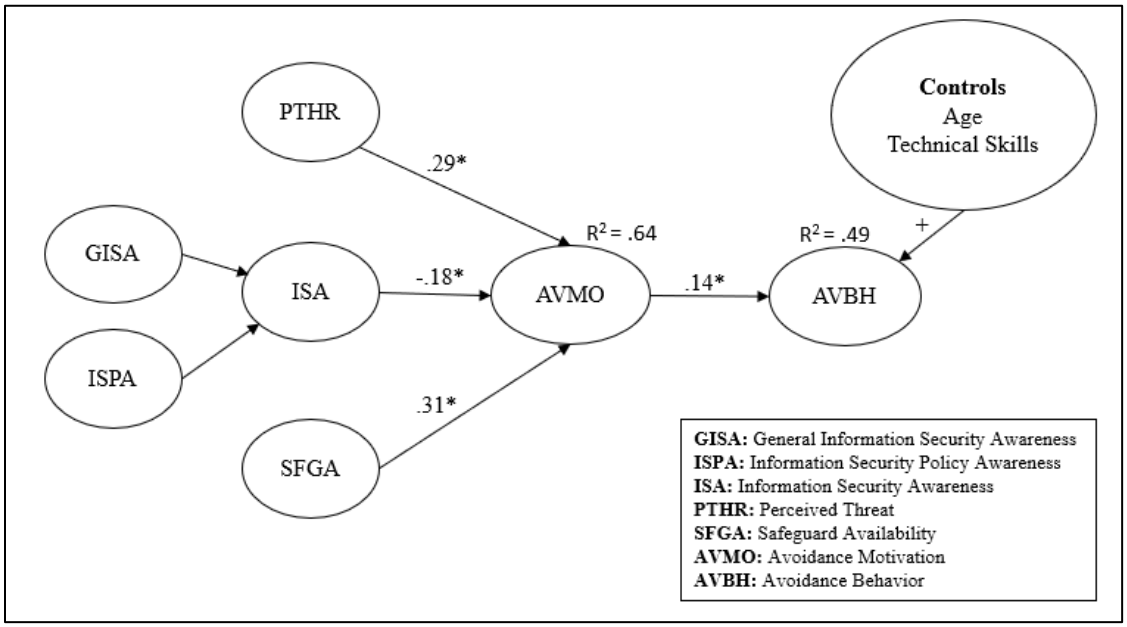

Fig. 2: Research Model Testing Results

Since ISA was conceptualized as a second-order construct formed by GISA and ISPA, the weights of these subdimensions were evaluated and were found to be significant ($t1 = 0.53$ and $t2 = 0.56$), which suggests that each subdimension significantly contributes to the underlying overall factor (Bulgurcu et al., 2010).

Discussion on Results

This study examines the effect of information security awareness on healthcare providers' motivations to avoid using the EMR based on the perceptions of risks and threats associated with using the EMR. The findings suggest that healthcare providers' ISA, which is formed by GISA and ISPA, has a negative direct effect on avoidance motivation, which implied that healthcare

providers who are aware about the security measures taken by the hospital to protect the data accessed by the EMR, are less likely motivated to avoid the EMR based on threat perceptions. Additionally, the study confirms the findings of previous research on technology resistance and avoidance (e.g., Samhan and Joshi, 2017; Bhattacherjee and Hikmet, 2007; Liang and Xue, 2010) by showing that perceived threat has a direct positive effect on avoidance motivation. This means, in the context of this study, the more healthcare providers view the EMR as a source of information security threats they will be motivated to avoid using it. Similarly, the availability of the safeguarding measure has a positive direct effect on avoidance motivation, which means that healthcare providers that are looking for a safeguarding measure will be motivated to avoid the EMR if they had one available and ready to use. For example, Samhan and Joshi (2017) reported that healthcare providers who perceived threats associated with the EMR were motivated to use a paper-based system for recording patients' data, in that example, healthcare providers considered the paper-based system as a safeguarding measure to avoid perceived threats.

Furthermore, the positive relationship between the avoidance motivation and behavior is confirmed. This suggest that higher levels of motivation to avoid the EMR will result in higher levels of EMR avoidance.

Age and technical skills had positive direct effects on the avoidance behavior. This has been confirmed in prior studies that considered evaluating the influcnece of age and self-efficacy on technology resistance or avoidance (Samhan and Joshi, 2017; Samhan, 2017; Kim and Kankanhalli, 2009).

Overall, based on data collected from 237 healthcare providers, all of the hypotheses were supported, and the findings show strong support for the hypothesized model.

CONTRIBUTIONS

This study makes several contributions to research. This work is considered one of the pioneer studies that examined the effect of information security awareness on mitigating technology avoidance behavior, especially in the healthcare context. Additionally, the study confirms the findings of the TTAT and ISPCT in a different context, which helps making these theories more generalizable to a variety of research contexts.

The study also provides several implications to practice. It provides a better understanding to what constructs predict EMR avoidance behavior and how could these behaviors be mitigated. Healthcare organizations invest heavily in implementing HIT and therefore these findings may be helpful for managers to understand how avoidance behavior may be mitigated to maximize the benefits stemming from using the HIT.

REFERENCES

1. Ajzen, I. 1991. "The Theory of Planned Behavior," Organizational Behavior and Human Decision Processes (50:2), pp. 179-211.
2. Ajzen, I., and Albarracin, D. 2007. "Chapter 1: Predicting and Changing Behavior: A Reasoned Action Approach," in Prediction and Change of Health Behavior: Applying the Reasoned Action Approach, I. Ajzen, D. Albarracin, and R. Hornik (eds.), Hillsdale, NJ: Lawrence Erlbaum & Associates, pp. 3-21.

3. Anderson, C. L. and R. Agarwal (2006) Practicing Safe Computing: Message Framing, Self-View, and Home Computer User Security Behavior Intentions, in *International Conference on Information Systems*, pp. 1543-1561. Milwaukee, WI.
4. Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304-312.
5. Bhattacherjee, A., and Hikmet, N. 2007. "Physicians' resistance toward healthcare information technologies: a dual-factor model." *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*, IEEE, 2007.
6. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, *34*(3), 523-548.
7. Carver, C. S. (2006). Approach, avoidance, and the self-regulation of affect and action. *Motivation and emotion*, *30*(2), 105-110.
8. Carver, C. S., & Scheier, M. F. (1982). Control theory: A useful conceptual framework for personality–social, clinical, and health psychology. Psychological bulletin, 92(1), 111.
9. Centers for Medicare and Medicaid services report (2017). Electronic Health Records incentives program. Retrieved Oct 12, 2017. https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html?redirect=/ehrincentiveprograms
10. Conner, M., and Armitage, C. J. 1998. "Extending the Theory of Planned Behaviour: A Review and Avenues for Further Research," Journal of Applied Social Psychology (28:15), pp. 1429-1464.
11. Cotea, C., 2010. "Electronic health record adoption: Perceived barriers and facilitators," *Centre for Military and Veterans' Health*, The University of Queensland.
12. D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research*, *20*(1), 79-98.
13. Edwards, J. R. (1992). A cybernetic theory of stress, coping, and well-being in organizations. Academy of management review, 17(2), 238-274.
14. Fishbein, M. 2008. "A Reasoned Action Approach to Health Promotion," Medical Decision Making (28:6), pp. 834-844. Fishbein, M., and Ajzen, I. 1975. Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research, Reading, MA: Addison-Wesley.
15. Freud, S. (1915) Repression, in, vol. XIVComplete psychological works of Sigmund Freud, London: Hogarth.
16. James, W. (1890) *The principles of psychology*. Vol. 2. New York: Henry Holt & Co.
17. Janz, N. K. and M. H. Becker (1984) "The health belief model: a decade later," Health Education Quarterly (11) 1, pp. 1-45.
18. Kim, H. W., & Kankanhalli, A. (2009). Investigating user resistance to information systems implementation: A status quo bias perspective. *MIS quarterly*, 567-582.
19. Lapointe, L., and Rivard, S., 2005. "A Multiple Model of Resistance to Information Technology Implementation", *MIS Quarterly*, 29, 3, pp. 461-491.
20. Lee, Y., & Kozar, K. A. (2008). An empirical investigation of anti-spyware software adoption: A multitheoretical perspective. *Information & Management*, *45*(2), 109-119.

21. Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: a theoretical perspective. *MIS quarterly*, 71-90.
22. Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7), 394.
23. Locasto, M. E., Ghosh, A. K., Jajodia, S., & Stavrou, A. (2011). The ephemeral legion: producing an expert cyber-security work force from thin air. *Communications of the ACM*, *54*(1), 129-131.
24. Maslow, A. H. (1943) "A Theory of Human Motivation," *Psychological Review* (50) 4, pp. 370-396.
25. Ng, B.-Y., A. Kankanhalli, and Y. C. Xu (2009) "Studying users' computer security behavior: A health belief perspective," *Decision Support System* (46) 4, pp. 815-825.
26. Rogers, R. W. (1975) "A protection motivation theory of fear appeals and attitude change," Journal of Psychology (91), pp. 93-114.
27. Rogers, R. W. (1983) Cognitive and physiological process in fear appeals and attitude change: a revised theory of protection motivation, in J. Cacioppo and R. Petty (Eds.) Social Psychophysiology: a source book, New York: Guilford Press, pp. 153-176.
28. Rosenstock, I. M. (1974) "The health belief model and preventive health behavior," *Health Education Monographs* (2pp. 354-386).
29. Samhan, B. (2016). *Why do people resist healthcare IT? Literature analysis, model testing, and refinement*. Washington State University.
30. Samhan, B. (2017, April). Security behaviors of healthcare providers using HIT outside of work: A technology threat avoidance perspective. In *Information and Communication Systems (ICICS), 2017 8th International Conference on* (pp. 342-347). IEEE.
31. Samhan, B., & Joshi, K. D. (2017). Understanding electronic health records resistance: a revealed causal mapping approach. *International Journal of Electronic Healthcare*, *9*(2-3), 100-128.
32. Sassen, E.J., 2009. "Love, hate, or indifference: How nurses really feel about the electronic health record system," *Computers, Informatics, Nursing*, 27(5), 281–287.
33. Security, in *International Conference on Information Systems*, pp. 367-380. Las Vegas, NV.
34. Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. *MIS quarterly*, 441-469.
35. The 2015 KPMG Healthcare Cybersecurity Survey. https://advisory.kpmg.us/content/dam/kpmg-advisory/PDFs/ManagementConsulting/2015/KPMG-2015- Cyber-Healthcare-Survey.pdf
36. The 5th Annual Benchmark Study on Privacy & Security of Healthcare Data. Ponemon Institute© Research Report. Sponsored by ID Experts - Independently conducted by Ponemon Institute LLC., Publication Date: May 2015. https://media.scmagazine.com/documents/121/healthcare_privacy_security_be_30019.pdf
37. Woon, I., G. W. Tan, and R. Low (2005) A Protection Motivation Theory Approach to Home Wireless.