5-1-2017

Organizational Challenges to Assimilating Security Policies and Practices in U.S. Healthcare Organizations

Kevin P. Gallagher
Cleveland State University, k.gallagher96@csuohio.edu

Xiaoni Zhang
Northern Kentucky University, zhangx@nku.edu

ORGANIZATIONAL CHALLENGES TO ASSIMILATING SECURITY POLICIES AND PRACTICES IN U.S. HEALTHCARE ORGANIZATIONS

Kevin P. Gallagher
Cleveland State University
k.gallagher96@csuohio.edu

Xiaoni Zhang
Northern Kentucky University
zhangx@nku.edu

Vickie Coleman Gallagher
Cleveland State University
v.c.gallagher@csuohio.edu

Abstract

This paper presents findings from a study of U.S. healthcare organizations and the role that their organizational challenges play in their efforts to fully deploy security-related measures. Specifically, we examined organizational antecedents of healthcare organization's assimilation of security policies and practices. The study examined perceived complexity related to the initiatives, the organization's compatibility with adopting and assimilating the measures, and the structure of the organization as measured by the degree of centralization and decentralization. As such, we examine the effect of complexity, compatibility, and centralization-decentralization on the assimilation of security-related measures. The model demonstrates that complexity related to the assimilation of security measures presents challenges for healthcare organizations, as it predicts lower levels of assimilation. Organizational compatibility and structure were not found to be significant. Our model controlled for the level to which these organizations had assimilated internet-related technologies and strategies in order to account for their level of sophistication with IT and their exposure to the risk of cyber threats. We conclude that complexity related to assimilation of security-related measures is a significant challenge.

Keywords:

IT Security, Policy Assimilation, Healthcare, Complexity

1. Introduction

Information technology (IT) is facilitating tremendous strides in the advancement of healthcare organizations and patient outcomes, as these institutions leverage patient data, increasingly sophisticated analysis, test results, and gain greater access to data-driven evidence-based decision making. Yet IT-related security issues continue to pose a tremendous threat to patient safety and security--ultimately a threat to the reputation and legitimacy of these organizations. Many studies conducted in recent years have examined the number and types of threats that organizations experience and their efforts to address these problems (Holmes, 2015-2016). Yet, as both the information technologies organizations use and the security measures they undertake continue to evolve, so too do the nature of threats. The escalating and evolving threats will surely leave ineffective today's solutions in combating tomorrow's threats.

Adoption of security measures are clearly an organizational challenge, as efforts are made to try and keep pace with technology and ever evolving threats. Furthermore, studying adoption of these security measures alone limits our ability to assess and understand the degree to which organizations have fully deployed these measures. Full deployment of new technology-based innovations that require changes to the organization's practices due to their complex nature are challenging (Attwell, 1992). Hence, this study examines security-related policies and practices as a complex organizational innovation (Attwell, 1992; Fichman & Kemerer, 2007) requiring adopting, deploying and assimilating security policies and practices. Assimilation is a more comprehensive method of analyzing the potential positive outcome of adopting and implementing IT-related innovations (Fichman & Kemerer, 2007) and has been used in prior studies of IT-related innovations in general, and within healthcare (Reardon & Davidson, 2007).

For healthcare organizations, security measures and related initiatives are particularly challenging, as many health care institutions work to adopt new technologies to their current organizational practices, while also developing new management practices and measures to leverage those innovations (Lian, Yen, & Wang, 2013). Existing and evolving regulations HIPPA regarding security and privacy creates challenges regarding the ability to safeguard patient data and insure privacy (Alrige, et al., 2014). Hence, healthcare provides a highly relevant industry to examine organizational challenges of assimilation.

We intend to understand the degree to which organizations have adopted and assimilated a set of measures to secure their information system, and then monitor and respond to security-related events. Thus, we study information security as an organizational concern to be managed through assimilation of effective policies and deployment of practices. While keeping pace with technology-based security measures are necessary, policies and practices enable organizations to more effectively plan, institute, and respond to security-related technology needs (Baskerville, 2008). Effective policies and procedures allow organizations the means to not only adopt and use effective IT security measures, but also diffuse newly adopted measures to respond to threats.

This study examines the organizational challenges to healthcare organizations assimilation of IT security-related policies and practices. Similar to adoption of other complex organizational innovations, assimilation of policies and practices can face difficult challenges. Organizations face challenges related to the complexities of adopting and fully deploying their work practices and procedures. Furthermore there are often initial losses in productivity that come with an organizational change and the changes to organizational norms and behaviors that have evolved with the organization's processes and routines. Changes in policies and practices could also mean that the organization would experience potential changes that conflict with existing organizational rules, decision-making processes, and locus of control of decision-making.

To examine the effect these organizational challenges pose for healthcare organizations, we develop and test a theoretical model based on existing organization-level measures of IT adoption. We modified these measures to not only examine the domain of IT-related security, but also extend our understanding beyond adoption to assimilation (e.g., full deployment). We tested the model using survey data collected from 64 healthcare organizations in the United States (U.S.). This paper will provide the theoretical background related to assimilation. We will outline the importance of our dependent variable, the antecedents of complexity, organizational

compatibility, and organizational structure, and end with our findings and a discussion of our contribution, limitations, and future research.

2. Theoretical Background

2.1. Importance of policies and practices

Information security policies and practices are vital to protect institutions and their resources; as such, policies and practices have attracted the attention of academic researchers (Straub, 2010). Policies and practices represent critical planning and control measures. The intent is to protect information, computer systems, and communications systems by outlining acceptable behaviors, establishing access protocols, defining system standards, and prescribing appropriate actions. In this research, we examine the deployment and use of these policies rather than specific technologies because we see them as more enduring. They represent an organizational mechanism for preventing security breaches and controlling its potential negative impact. Information technology, its adoption by healthcare organizations, and the nature of security threats and technology-related safeguards, all continue to evolve. This evolution has accelerated in recent years in the healthcare industry, in part due to the implementation of the Affordable Care Act. Furthermore, the adoption of technologies related to the internet have also raised the need for all organizations, including those related to healthcare, to increase their capabilities related to information technology and the overall information security of the organizations. While many surveys are conducted with the intention of tracking specific technologies and applications, the insights gleaned from these studies have a limited time horizon, given the time required to collect and report the findings of a study such as this. That is, these technologies are likely to become outdated before the manuscript is published.

If organizations are to safeguard their information and systems, then effective IT security measures must go beyond the adoption and use of security-related technologies and applications. Security measures must insure appropriate training, monitoring, and responses to breaches (Puhakainen & Siponen, 2010). More so, a comprehensive set of security policies and measures can that personnel are aware, trained and guided to evaluate security related situations.

However, there are many challenges to the comprehensive creation and implementation of security policies and practices (Warkentin & Johnson, 2008). Importantly, policies and practices may be adopted, but as with any innovation, it may not be fully utilized. Even when there is compliance, interpretation of policies can be an obstacle to their effective implementation and execution (Warkentin & Wilson, 2009). Finally, feedback and monitoring is necessary to safeguard the systems and improve on the policies and practices (Warkentin & Wilson, 2009), to illuminate the need to update policies based on emerging problems and evolving needs.

2.2. Assimilation of Security policies and practices

Assimilation is a way to measure the degree to which an organization has not just made a decision to adopt, but has fully deployed the policies in measures (Cho & Kim, 2001/2002). For example, in the case of a security-related policy, it might take some education, experience and perhaps mandatory rules in order to insure that the policy's guidelines are understood and procedures followed. In fact, Fichman and Kemerer (2007) introduced the concept of assimilation in the management literature as a way to explore what they described as the illusory experience of organizations with innovation adoption. The complex organizational challenge that they examined was the adoption of programming methods, which requires not just new

technology, but new knowledge, changes in work processes, and changes in organizational procedures. The authors found that a broader range and depth of experience related to information technologies led to greater levels of assimilation. They also found that greater related knowledge in the organization lead to higher levels of assimilation, as workers had access to the experience and expertise they needed to help them through the learning process.

Fichman and Kemerer (2007) studied assimilation with regard to the deployment of the innovation in question. Recognizing that innovations differ, they authors noted that future studies of assimilation should consider the characteristics of the particular innovation under study. Thus, Reardon and Davidson (2007), recently studied adoption and use of electronic medical records in small physician practices. The challenges of this innovation and the existing context of the organizations was very different; hence, the antecedent conditions that might predict higher levels of assimilating the innovation, such as the related knowledge, were suggested.

Assimilation has historically been studied as a dependent variable. It serves to inform and measure an organization's adoption of an innovation. Viewing security policies and practices as a complex organizational innovation, we believe the approach undertaken by Armstrong and Sambamurthy (1999) provides a means to measure, as a dependent variable, the range of policies and practices that an organization has deployed, and the degree they are fully implemented.

2.3. Security policies and practices viewed as complex organizational innovations

In this research, and as noted above, we conceptualize the adoption of security-related policies as a complex organizational innovation that must be assimilated to insure its effectiveness. The acquisition of an innovation alone cannot insure its full deployment or use (Fichman & Kemerer, 2007). Therefore, a more important measure of an organization's deployment of such innovations is the degree to which it is assimilated (Armstrong & Sambamurthy, 1999; Fichman & Kemerer, 2007; Reardon & Davidson, 2007).

Studies of innovation have often examined the challenges that constrain adoption, as well as those things that might enable higher levels of adoption, examining both the characteristics of the innovations themselves, as well as the characteristics of the organizations (Damonpour, 1991; Rogers, 1995). Ultimately, some aspects of adoption are a product of both the innovation and the organization, given the organization's assessment of the innovation will be undertaken with regard to the costs, challenges, and benefits associated with adoption (Rogers, 1995).

Complexity of the innovation being adopted can pose challenges for the organization, but more so, the complexity of instituting the initiatives can make it difficult. This makes the complexity both a product of the innovation and the organization (its knowledge, capabilities, and experience with similar innovations). Thus, the challenge is directly inherent in the innovation, but also related to the organization's knowledge based on its prior experience, i.e. absorptive capacity (Cohen & Levinthal, 1990). As a result, greater relative complexity has been found to lower levels of adoption and the ability to fully assimilate innovations (Rogers, 1995).

From a security perspective, greater relative complexity of security policies and procedures might inhibit understanding them from multiple perspectives, including business, technical, and work processes. For example, greater perceived complexity could be viewed as potentially hampering the ability to monitor and resolve IT-related problems that support business

processes, or to support ongoing work practices to insure healthcare professionals the ability to access data and support users and patient needs. Thus, complexity is multifaceted. The compatibility of the innovation has also been examined in many past studies of innovation, including those examining IT-related innovations (Jones & Beatty, 1998). Compatibility is associated with higher levels of adoption; however, lower levels or complexity are viewed as creating challenges, thus predicting lower levels of adoption. The incompatibility of the innovation is realized or experienced within the organization by a greater degree of initial disruption caused by the introduction of the innovation. Such problems would also result in losses in productivity, or experienced as changes in organizational values, norms, and culture, as the demands of the innovation conflict with the management of the organization.

Another organizational challenge might be the existing organizational structure (Daft, 2010). Prior research has shown that structure can enable or constrain the progress of policy development and implementation of practices (Warkentin & Johnson, 2008). Organizational structures determine the locus of control and decision making in an organization, impacting adoption of IT-related initiatives. For example, a practice that requires a standardized set of policies and rules, can become more challenging when a decentralized organization exists.

Based on the above review of relevant antecedents to adoption and assimilation, healthcare organizations are likely to exhibit similar challenges, given the complex nature of the work they undertake and the sensitive nature of the data they are collecting, storing, and analyzing. However, these organizations have additional challenges because many are also in the midst of installing new technologies within their work practices and procedures as they try to keep pace with the demands from stakeholders. Healthcare organizations are likely be impacted by complexity, compatibility, as well as structure, as they deploy security-related measures.

Finally, it is important to recognize that if the organization is more advanced in its use of the technologies like the internet, this would exhibit their greater sophistication with IT, and would also potentially lead to a raised level of concern regarding the organization's potential security exposure. As such, we propose the following model and the requisite hypotheses development.

3. Research model and hypothesis development

3.1. Dependent variable

We conceptualize security-related policies as a complex undertaking requiring its full deployment, or assimilation, not just adoption. It is assimilation that helps organizations reduce the impact of security breaches. Our research model is illustrated in Figure 1. As with other studies that have attempted to examine and measure higher levels of organizational deployment beyond adoption (Reardon & Davidson, 2007), and suggested by Fichman and Kemerer (2007), we undertook a conceptual translation of an assimilation measure put forth by Armstrong and Sambamurthy (1999). Our conceptualization is an effort to study a different, yet complex innovation, and its adoption into an organizational context. The aforementioned authors asked respondents to evaluate their organization's application of IT in a series of activities related to IT adoption relative to others in their industry. Similarly, we utilized their measure by asking the same question, only related to security rather than IT. Furthermore, we adapted the activities to reflect security-related activities, rather than value chain, as employed in the original measure.

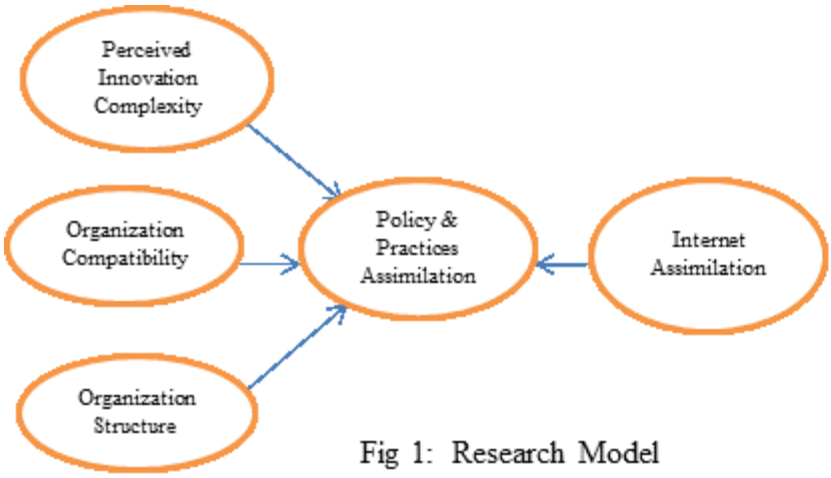

Fig 1: Research Model

3.2. Antecedent variables

To examine the organizational challenges that might limit the adoption and assimilation of security measures, we theorize three constraints; the perceived complexity of the initiative itself, in this case instituting security-related measures, the organization's compatibility with the change being instituted, and the organization's structure.

Complexity of an innovation has been studied in the past to understand levels of adoption, and in particular, as an inhibitor to adoption in organizations (Grover, 1993; Tornatzky & Klein, 1982). However, the theoretical undertaking here, and the conceptualization in the assimilation literature, is that the perceived level of complexity for an innovation is as much a function of the organization, its experiences, knowledge, and know-how, as it is a function of the innovation itself. Based in organizational learning theories, adoption of past complex organizational innovations helps organizations develop bundles of knowledge and capabilities that allow them greater abilities to recognize, understand, and adopt future complex innovations. Thus, they develop greater absorptive capacity (Cohen & Levinthal, 1990), which allows them to assimilate innovation at greater levels (Fichman & Kemerer, 2007). When organizations are not as versed and experienced with innovations, they will find them less familiar and more complex, which should lead to less initiatives in the organization and generally lower levels of assimilation (Teo, Wei, & Banbasat, 2003). Thus, our first hypothesis predicts that greater perceived complexity will lead to lower levels of assimilation of security-related policies and practices.

> **H1:** Greater perceived complexity on an innovation will lead to lower levels of assimilation of security-related policies and practices.

Organizations also examine innovations with regard to their compatibility with various dimensions of the organization. These dimensions may be related to the innovation's business value or how existing work practices might fit with the innovation and its design (Jones & Beatty, 1998). However, organizations may not always effectively evaluate the compatibility, or delays in the implementation or an innovations life cycle can alter degrees of compatibility, resulting in a misfit. Furthermore, when a complex organizational innovation is mandated, or absolutely necessitated (in spite of the organization's assessment that there is a lack of fit with existing work practices or its business value), then adoption can move forward regardless of fit.

The organization will then face difficult challenges. For example, adoption of innovations can face a productivity dip during the initial implementation. Such difficulties could be exacerbated if challenges related to compatibility are ignored. Similarly, ignoring an innovation's conflict with an organizations values, beliefs or norms could also create difficult challenges during the innovation's adoption and implementation. When this occurs, it can create challenges for the adopting organization that can lead to reduced levels of the innovation's assimilation.

> **H2:** Greater levels of an innovations compatibility with the organization will lead to higher levels of assimilation of security-related policies and practices.

Organization structures can vary from highly centralized, where control and decision making are known and understood to reside in a central individual or office, to highly decentralized, where decision making and control are dispersed, allowing for localized adaptation and autonomy amongst managers or operational practices. Each structure has advantages and disadvantages (Sambamurthy & Zmud, 1999). For example, a highly centralized organization structure has certain efficiencies associated with the standardization of task activities and procedures. Alternatively, a highly decentralized organizational structure may be less efficient, but can promote greater levels of experimentation and innovation. For the adoption of a complex organizational innovation like IT-related security measures, which involve adoption and adherence to a prescribed set of policies and practices, a decentralized organizational structure could confront enhanced levels of variation in existing work practices and procedures, which could necessitate greater levels of effort in adopting and implementing the policies and practices. Thus, a decentralized organization structure should create greater challenges for assimilating security-related measures, relative to a centralized structure.

> **H3:** Greater decentralization of an organization's structure will lead to lower levels of assimilation of security-related policies and practices.

3.3. Control variable

All three of the antecedent variables are theoretically based in an organization's capabilities, relative to its prior adoption of complex innovation, its ability to assess and address issues of compatibility, and the ability to execute given its existing structure. Furthermore, the concept of assimilation recognizes the difficulties organizations have in not just adopting, but then using and gaining the benefits of an innovation. Fichman and Kemerer (2007) stated that organizations were more likely to assimilate such complex organizational innovations when there was a greater scale of activities over which the learning required to assimilate the innovation could be spread. Conceptually, greater scale of activities benefits from economies of scale (Fichman & Kemerer, 2007). Furthermore, they state that greater diversity of technical knowledge and activities would also lead to greater assimilation. Theoretically, greater diversity benefits from an organization having greater absorptive capacity (Cohen & Levinthal, 1990).

To measure scale and diversity of activities that might lead to an organization assimilating a set of security-related policies, we believe we should consider an organization's assimilation of internet-related strategies and activities. Experience with the internet and technology leads to potentially greater needs and motivations to protect against the adverse effects of security breaches. To measure internet-related capability, we adopt an existing internet assimilation scale that examines both strategies and activities (Chatterjee, Grewal, & Sambamurthy, 2002),

Strategies include offering value-added services, etc. Activities include receiving payments, delivering services, etc. (see measures below).

Interestingly, one could argue that organizations that have assimilated a broader range of strategies and activities via the internet are presented with a greater level of risk for security breaches. Specifically, their internet presence makes a larger audience aware of their website and a more extensive set of activities offers more opportunities for a breach. Thus, greater assimilation of both internet strategies and activities could lead to greater exposure to breaches.

Similarly, as organizations gain greater experience and knowledge of these internet-related strategies and activities they should become increasingly aware of the need for security related policies in order to protect their organization, its systems data, and reputation. They should also come to understand that not having these systems available to their customers, suppliers and partners, creates a disruption in their operation that can be costly. As such, we included internet related capabilities as a control variable.

4. Research methods and analysis

4.1. Sample and data collection

Development of the model and examination of the organizational challenges for healthcare organizations was undertaken as part of a larger study of the state of IT security and adoption of security-related policies and practices in U.S. The majority of the survey data were collected from individuals in organizations using existing survey panel members solicited through a market research vendor, with members screened to identify participants who fit a number of requirements: region, industry, etc. Participation was requested through an email invitation. To insure that participants were qualified, we used several forms of screening and validation. First, the survey panel was mined for respondents who were decision makers, had knowledge of IT and were managers in their organizations. Secondly, we asked screener questions about requisite knowledge of security issues within their company (e.g., policies, practices, and management of IT). The sub-sample analyzed to test this model of healthcare organizations consists of 64 responses in a wide range of geographic locations across the country and company size.

4.2. Measures

4.2.1. Assimilation of policies and practices. Similarly to other studies of assimilation of complex organizational innovation (Reardon & Davidson, 2007), we adapted a measure to suit the context of our innovation. In this case we adapted a measure employed by Armstrong and Sambamurthy (1999), in order to study a complex innovation's, organizational adoption. We asked respondents to evaluate an organization's application of series of activities related to security, in their industry. We adapted their measure by asking the same question, but adapted them to reflect security-related activities. The scale's responses ranged from 1 to 7 as follow: 1) Poor, 4) Average, 7) Excellent. We created a multi-item scale composed of four security-related policies and practice activities, including documenting policies and practices, implementing measures to safeguard assets, monitoring for breaches, and gaining user compliance.

4.2.2. Perceived Innovation Complexity This construct measures the degree to which an innovation is perceived as relatively difficult to understand and use (Rogers, 1995). We adapted this scale from a study of adoption of inter-organizational linkages by Teo et al. (2003), again adapting it to the specific context of the innovation. Thus, we asked about the complexity of

instituting information security measures with eight items. The scale's responses ranged from 1 to 7 as follow: 1) Strongly disagree, 4) Neutral, 7) Strongly agree.

4.2.3. Organization compatibility Again, we adapted the measure to reflect the context of the innovation under study. We adapted our measure of organizational compatibility from a study of enterprise systems assimilation (Liang, Saraf, Hu, & Zue, 2007). In doing so, we asked respondents to report the extent to which adoption of information security related practices affected their organization. As with Liang et al., our measure had three items. The scale's responses ranged from 1 to 7 as follow: 1) Strongly disagree, 4) Neutral, 7) Strongly agree.

4.2.4. Organizational structure To measure the organizational structure, we adapted a scale previously used in a published study of organizational structure and ERP implementation (Gallagher and Gallagher 2013). The scale asked respondents to provide their indication along a range of option using a scale from 1 to 0, with 1 being centralized and 9 decentralized.

4.2.5. Internet-related capabilities Web activities and strategy measures the extent and depth to which an organization has assimilated web-based technologies to advance its business activities and strategy. Five items were used to measure web strategy (e.g., company website supports enhancing the company image). The five items were adapted from Chatterjee et al.'s study (Chaterjee, Grewal, & Sambamurthy, 2002). One item was deleted after confirmatory analysis.

4.3. Data analysis

4.3.1 Sample and Data Collection The sample analyzed consists of 64 responses in healthcare organizations. The average number of employees of the healthcare organizations sampled is 1080. Table 1 shows descriptive statistics and reliabilities. Reliability scores range from 0.81 to 0.97, exceeding the recommended threshold of 0.79 (Robinson, Shaver & Wrightman, 1991).

	Mean	Std. Deviation	Reliability
Compatibility	4.5703	1.46620	0.81
WebAssimilation	4.3438	1.51337	0.91
Complexity	4.4648	1.58701	0.97
Security Practice	4.9766	1.37849	0.92

Table 1 Descriptive Statistics and Reliability

5.3.2 Measurement Model AMOS 21 was used for the confirmatory analysis on the factors and the test of hypotheses. Table 2 shows the loadings of the CFA. The loadings in table 2 are in the range of 0.75 and 0.94, greater than the suggested value of 0.5 (Straub, 1989). The fit indices for the measurement model is GFI =0.83, CFI=0.96, CMIN/df=1.34, RMSEA=0.07. These indices indicate good model fit and provide evidence of both convergent validity and unidimensionality (Bagozzi, Yi, & Phillips, 1991; Gerbing & Anderson, 1988). In addition, as shown in Table 2 high and significant factor loadings provides further evidence of convergent validity.

		Loadings
Complexity	QD10F	0.89
	QD10E	0.89
	QD10D	0.93
	QD10C	0.84
	QD10B	0.85
	QD10A	0.91
	QD10G	0.94

	QD10H	0.90
OrgCompatable	QD11A	0.75
	QD11B	0.91
Security Practice	QD12A	0.87
	QD12B	0.91
	QD12C	0.84
	QD12D	0.82

Table 2 Factor Loadings

Table 3 shows item-to-construct correlations. Each item correlates highly with its intended construct than with others. The item-to-construction correlations provide evidence of both convergent and discriminant validity (Fornell & Larcker, 1981).

4.3.3 Structural Model The fit indices for the structural model are GFI=0.92, CMIN/df=2.77, CFI=0.87. These fit indices show good model fit to the data. Figure 2 shows the significant path coefficients. The dashed lines are insignificant paths. When using complexity and organization compatibility as independent variables to predict security practice controlling for degree of centralization and web assimilation, R square is 47%. (See Figure 2 below Table 3.)

	Complexity	Security Practices	Org Compatibility
QD10A	**.93**	.06	.52
QD10B	**.88**	.04	.47
QD10C	**.87**	-.01	.46
QD10D	**.93**	-.02	.60
QD10E	**.90**	-.06	.51
QD10F	**.90**	.00	.49
QD10G	**.94**	.08	.56
QD10H	**.91**	.04	.45
QD11A	.47	.19	**.92**
QD11B	.56	.21	**.91**
QD12A	.00	**.90**	.25
QD12B	.06	**.92**	.22
QD12C	.06	**.89**	.20
QD12D	-.03	**.88**	.12

Table 3 Item-to-Construct Correlations

Organization compatibility and degree of centralization do not have significant impact on security practices. Complexity has a negative impact on security practice. When healthcare organizations are perceived more complex, their security practices are worse.

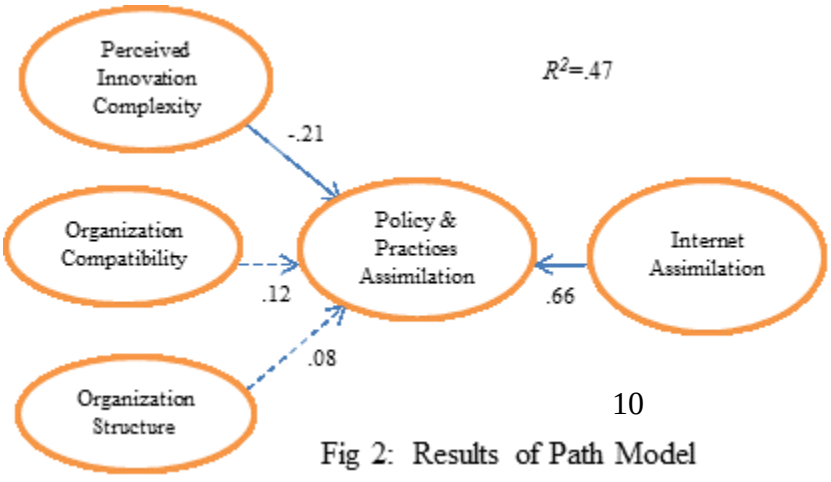

Fig 2: Results of Path Model

5. Discussion

Rather than address the continuous technological arms race, our research addresses an important aspect of information security: the deployment and assimilation of policies and practices. Policies and practices are a vital mechanism in planning and control in order to protect valued resources against security threats. An important contribution of our research is that we study the challenges to healthcare organizations assimilating policies and practices. We study policies and practices because we see their assimilation as a systemic solution, designed to address existing and emerging threats over time, regardless of the technology or technique used in the breach.

An important contribution of our study is that we tested and confirmed all three independent variables. Although a number of factors are likely to constrain the adoption and assimilation of policies and practices, we hypothesized that three specific challenges could potentially suppress levels of policy and practices assimilation. Interestingly, only complexity was found to be significant in our sample, with higher levels of perceived complexity leading to lower levels of assimilation of security-related policies and practices, as hypothesized. The direction of the other two independent variables was as hypothesized, although the relationship was not found to be significant in this sample of healthcare organizations. Prior research had offered contradictions with regard to the relationships between organizational structure and adoption of innovations.

The primary limitations of our study are related to potential limits of our data collection and our sample size. Our data set has just 64 organizations. Nevertheless, we have a good mixture of organizational sizes represented. This being a cross-sectional survey, we collected responses to all questions at the same time. A longitudinal study in the future is therefore recommended. In fact, several areas of future research can be derived from the discussion and limitations outlined above. First, we hope to examine larger samples in the future. Second, we intend to conduct further analysis regarding the high correlation of our control variable, internet assimilation, with our dependent variable. This may be a product of our small samples size in the healthcare industry. We hope to analyze this relationship within other industries. Third, we wish to explore possible interviews with survey participants to understand how the organizational challenge we investigated here influence organization's assimilation of policies and procedures.

References

Alrige, M., Alsudais, A., Plachkinova, M., Chatterjee, S., Edwards, A., Edwards, J., & Weinstein, A. (2014). EHR Adoption in Healthcare Practices: Lessons from Two Case Studies, *Proceedings of the Twentieth Americas Conference on Information Systems*, Savannah, GA, 2014.

Armstrong, C.P. & Sambamurthy, V. (1999). Information Technology Assimilation in Firms: The Influence of Senior Leadership and IT Infrastructures, *Information Systems Research*, *10*(4), 304-327.

Attwell, P. (1992). Technology diffusion and organizational learning: The case of business computing, *Organization Science*, *3*(1), 1-19.

Bagozzi, R., Yi, Y., & Phillips, L.W. (1991). Assessing Construct Validity in Organizational Research, *Administrative Science Quarterly, 36*, 421-458.

Baskerville, R.L. (2008). Strategic Information Security Risk Management, In *Information Security Policies and Practices,* Straub D., Goodman S. & Baskerville, R.L. Eds., M.E. Sharpe, Armonk, NY, 112-122

Chatterjee, D., Grewal, R., & Sambamurthy, V. (2002). Shaping up for e-commerce: Institutional enablers of the organizational assimilation of web technologies, *MIS Quarterly*, *26*(2), 65-89.

Cho, I. & Kim, Y. (2001/2002). Critical Factors for Assimilation of Object-Oriented Programming Languages, *Journal of Management Information Systems*, *18*(3), 125-156.

Cohen, W. M. & Levinthal, D. A. (1990). Absorptive Capacity: A New Perspective on Learning and Innovation, *Administrative Science Quarterly, 35,* 128-152.

Daft, R.L. (2010). Organization Theory and Design, *South-Western Cengage Learning,* Mason, Ohio.

Damonpour, F. (1991). Organizational Innovation. A Meta-Analysis of Effects of Determinants and Moderators, *Academy of management Journal, 34*(3), 583-613.

Fichman, R.G. & Kemerer, C.F. (2007). The Assimilation of Software Process Innovations: An Organizational Learning Perspective, *Management Science, 43*(10), 345-1363.

Fornell, C. & Larcker, D.F. (1981). Evaluating Structural Equation Models With Unobservable Variables And Measurement Error, *Journal of Marketing Research, 18*(1), 39–50.

Gallagher, KG & Gallagher, V.C., Organizing for Post-Implementation ERP: A Contingency Theory Perspective, *Journal of Enterprise Information Management,* 25, 2, 2012, pp 170-185.

Gerbing, D.W. & Anderson, J.C. (1988). An Updated Paradigm for Scale Development Incorporating Unidimensionality and Its Assessment, *Journal of Marketing Research, 25*, 186-192.

Grover, V. (1993). An Empirically Derived Model for the Adoption of Customer-Based Interorganizational Systems, *Decision Sciences*, *24*(3), 603-640.

Holmes, A. (2015-2016). The Global State of Information Security, *PWC*, http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html.

Jones, M.C. & Beatty, R.C. (1998). Toward the Development of Measures of Perceived Benefits and Compatibility of EDI: A Comparative Assessment of competing first Order Factor Models, *European Journal of Information Systems, 7*(3), 210-220.

Lian, J., Yen, D.C., & Wang, Y. (2013). An Exploratory Study to Understand the Critical Factors Affecting the Decision to Adopt Cloud Computing in Taiwan Hospitals, *International Journal of Information Management, 34,* 28-36..

Liang, H., Saraf, H., Hu, Q. & Xue, Y. (2007). Assimilation of Enterprise Systems: The Effect of Institutional Pressures and the Mediating Role of Top Management, *MIS Quarterly, 31*(1), 59-87.

Puhakainen, P. & Siponen, M. (2010). Improving Employees' Compliance through Information Systems Security Training: An Action Research Study, *MIS Quarterly, 34*(4), 757-778.

Reardon, J.L., & Davidson, E. (2007). An Organizational Learning Perspective on the Assimilation of Electronic Medical Records among Small Physician Practices, *European Journal of Information Systems, 16,* 681-694.

Robinson, J. P., Shaver, P. R. & Wrightman, L. S. (1991) Criteria for Scale Selection and Evaluation, in Measures of Personality and Social Psychological Attitudes. San Diego,

CA: Academic.
Rogers. E.M. (1995). Diffusion of Innovations, *Free Press*, New York.
Straub, D., Ed. (2010). Special Issue: Information Systems Security, *MIS Quarterly, 34*(3).
Teo, H.H., Wei, K.K. & Banbasat, I. (2003). Predicting Intention to Adopt Interorganizational Linkages: An Institutional Perspective, *MIS Quarterly*, *27*(1), 19-49.
Tornatzky, L.G. & Klein, K. (1982). Innovation Characteristics and Innovation Implementation: A Meta-Analysis of Findings, *IEEE Transactions on Engineering Management, 29*(1), 28-45.
Warkentin, M. & Johnston, A.C. (2008). IT Governance and Organizational Development for Security Management, in *Information Security: Policies, Processes, and Practices*, Straub D., Goodman S. & Baskerville, R.L. Eds, M.E. Sharpe, Armonk, NY, 46-68.
Warkentin, M. & Wilson, R. (2009). Behavioral and Policy Issues in Information Systems Security: The Insider Threat, *European Journal of Information Systems*, 18, 201-105.
Sambamurthy, V. and Zmud, R.W. (1999), "Arrangements for information technology governance: a theory of multiple contingencies", MIS Quarterly, 23m 2, pp. 261-91.