Security Failure in Electronic Health Record Systems: The Influence of Meaningful-use and IT Security Investment

Emergent Research Forum (ERF) Papers

Amin Shoja
Florida International University
ashoja@fiu.edu

George M Marakas
Florida International University
gmarakas@fiu.edu

Abstract

This research draws upon the institutional theory and strategic IT adoption of organizations to examine the influence of meaningful-use of EHR systems and IT security investments on the likelihood of data breaches in hospitals. We expect that the intensity of such a relationship depends on hospitals symbolic or substantive adoption approaches. Mainly, we believe that organizations with symbolic adoption approach face a higher risk of security failures. Hospitals with (i) more complementary IT applications such as financial systems, scheduling systems, and HR systems, (ii) not-for-profit, and (iii) teaching and faith-oriented hospitals are less likely to classify as symbolic adopters. For that purpose, this paper takes advantage of unique data sets which provides detailed information on EHR system adoption by hospitals as well as the majority of data breaches. Further, we identify changes in the likelihood of breach performance consequent to meaningful-use and IT investment by employing Fixed-effect panel analysis and propensity score matching approach.

Keywords

Health IT, data security breaches, IT security, institutional theory, electronic health record systems

Introduction

Information technology (IT) system adoption and infusion of that technology are central issues in the organizational literature (Cooper & Zmud, 1990; Agarwal & Prasad, 1998). From the health IT perspective, the use of Electronic Health Record (EHR) systems is becoming more widespread and is replacing the use of paper records. Thus, addressing security, privacy, and confidentiality issues is one of the core subjects not only for hospitals and healthcare providers but also for health IT researchers (Angst et al., 2017; Kwon & Johnson, 2014).

EHR systems’ characteristics such as showing real-time changes and being patient-centered records, increase the adoption value of these systems by hospitals and improve patient-care (Blumenthal & Tavenner, 2010). Furthermore, this allows health information to be available instantly to all authorized EHR’s primary stakeholders including patients, providers, and purveyors (Kohli and Tan, 2016). Yet, for healthcare providers, lack of appropriate security protocols exposes them to higher risk of data breaches (Jha et al., 2009). In this regard, many healthcare providers have attempted to meet minimum standards required for “meaningful-use” certification and security has not been the priority, until recently (2018 HIMSS Cybersecurity Survey).

Under the Health Information Technology for Economic and Clinical Health (HITECH) act, the department of health and human services released the final criteria defining stage 1 “meaningful-use” of EHR systems for hospitals to receive financial incentives (Jha, 2010). To meet stage 1 meaningful-use criteria for formal attestation, a healthcare provider was entitled as having a basic EHR system if it identified and implemented ten specific electronic clinical functions (Jha et al., 2009). These electronic
clinical functions include electronic clinical documentation, results viewing, and computerized provider order entry.¹

However, there are concerns that this formal certification motivated by economic subsidies and incentives is not always associated with actual improvement in organizational efficiency and tempt organizations to just meet the meaningful-use criteria for formal attestation (Carlos & Lewis, 2018; Puhakainen & Siponen, 2010). This approach focuses on meeting the minimum standards required for meaningful-use certification and may meet the basic security concerns. However, this approach would hardly satisfy the necessary security requirements to prevent data breaches. Consequently, while organizations attain formal attestation, still poorly integrated EHR systems and ill-designed security protocols are in the core of these data breaches (Yasnoff et al., 2013).

Our motivation comes from studies such as Kwon & Johnson, 2014 and Angst et al., 2017 who investigated the effect of basic meaningful-use attestation or IT security investment on the likelihood of data breaches in U.S. healthcare industry. Yet, there is concern that the adoption of meaningful-use is not always associated with actual improvement in organizational efficiency (Carlos & Lewis, 2018). Benefits of formal legitimacy may incorporate to receive incentive payments for meaningful-use of EHR systems. However, this formal legitimate adoption (mandated by legislation) is not always associated with desired outcomes or performances. In this case, data security breaches in hospitals from internal failures and external risks are threatening the organizational efficiency and patients’ privacy and security. To attain desired outcomes or performances, organizations often have substantive adoption approach. The present study attempts to offer further explanations on how two strategic IT adoption classes, symbolic or substantive adoption, can explain the likelihood of such security failure. Organizations with symbolic EHR adoption approach (as opposed to substantive EHR adoption approach) are assumed to meet the minimum criteria to the extent to which they gain the short-term financial benefits.

This paper particularly examines the importance of the strategic decision of EHR system adoption under security failure risks in the U.S. healthcare sector. With employing a rich longitudinal panel data set of hospitals, we explore the likelihood of healthcare data breaches through meaningful-use and IT security investment in EHR system adoption. Further, this study uses the two strategic IT adoption approaches including symbolic or substantive adoption to explore such a likelihood. Hospitals with (i) more complementary IT applications such as financial systems, scheduling systems, and HR systems, (ii) not-for-profit business model, and (iii) Academic or teaching based and faith-oriented hospitals are less likely to classify as symbolic adopters. Understanding the likelihood of data security breaches in hospitals would be critical not only for hospitals and healthcare providers in terms of the process of making future business strategic decisions but also for policymakers for designing legislation to improve the industry as a whole.

**Theoretical Foundation and Hypotheses**

The Institutional theory focuses on how organizations are influenced by the social environment and by the norms and values of their institutional context (DiMaggio & Powell, 1983; Scott, 1987). The key point is that there are other higher order structures (institutional rules) that dominate the rationality of organizations to follow their optimal actions. Instead, organizations get the benefit when their actions are recognized as legitimate. The organizations are then forced to follow the norms and values of their institutional setting to get the benefit of legitimacy such as enhanced access to resources and support, increase in customer acceptance, and reduce the risk of business failure (Pfeffer & Salancik, 1978).

Additionally, hospitals adopt different levels of new IT practices to maintain their internal flexibility (DiMaggio & Powell, 1983). Hospitals can keep their cost at low levels by adopting practices symbolically and avoid the cost of full practices of EHR systems. Obvious consequences of such an ill-designed and poorly integrated EHR systems could lead to security issues and possible data breaches. This paper takes

---

¹ Functions included in a Basic EHR meaningful-use attestation: Patient demographics, Physician notes, Nursing Assessments, Problem lists, Medication lists, Discharge summaries, Lab reports, Radiology reports, Diagnostic test results, and Medications order entry
advantage of the concept of symbolic or substantive adoption based on the institutional theory and explains how hospitals communicate their legitimacy through sending signals.

There are key concepts present in this theory which can be employed in health IT context to explain the signaling notion by hospitals further. This distinction between symbolic or substantive adoption based on the institutional theory can help explain why meaningful-use or IT security investment in EHR systems have not been entirely effective and how the healthcare industry suffers from high rates of data breaches. Information technologies must become routinized and technological complementarity should be considered on organizations’ investment behavior and business strategies before they can become valuable assets in business activities (Cooper and Zmud, 1990). The literature suggests that such routinization and technological complementarity could be a significant factor in IT adoption (Boynton et al. 1994; Azevedo and Paxson 2009). Organizations who are avoiding the cost of necessary implementation by decoupling practices will not get the desired outcomes although some hospitals follow such practices to gain short-term financial benefits.

Previous studies attempted to classify symbolic and substantive adopters based on characteristics such as hospital age, hospital size, business model, teaching or faith-based oriented, and entrepreneurial orientation (Angst et al., 2017). In this study, we take advantage of characteristics such as coupling more complementary IT applications such as financial systems, scheduling systems, and HR systems to characterize such classification and keep for-profit or not-for-profit, teaching or faith-based oriented as well (Figure 1). Since decoupling such complimentary practices to avoid the cost of substantive adoption for short-term gains is at the center of this notion, we believe such model specification will help to explain the notion of symbolic and substantive adoption better. As discussed before, by decoupling complementary practices, organizations will not get the desired outcomes. Further, we can argue that hospitals with non-profit business models less likely focus on short-term benefits and based on that logic, less likely to follow symbolic adoption to deliver higher profits (Shin et al. 2012). On the other hand, academic or teaching based oriented hospitals are more likely substantive adopters due to the higher priority in consumer preferences based on their mission and business core identity. Hence, the following hypothesis:

H1.a: for-profit hospitals are more likely to be symbolic adopters.

H1.b: hospitals with less IT applications such as financial systems are more likely to be symbolic adopters.

H1.c: hospitals with less IT applications such as scheduling systems are more likely to be symbolic adopters.

H1.d: hospitals with less IT applications such as HR systems are more likely to be symbolic adopters.

H1.e: teaching hospitals are less likely to be symbolic adopters.

H1.f: faith-based hospitals are less likely to be symbolic adopters.

![Figure 1: Predictors of Symbolic or Substantive Adoption](image)

Figure 2 shows our conceptual model of the influence of IT security investment and EHR meaningful-use on the likelihood of data breaches, moderated by symbolic or substantive adoption. While we use variables such as hospital age, hospital size, and the number of beds as control variables in our model specification. Hence, the following hypothesis:

H2: the relationship between IT security investment and the likelihood of data breaches will significantly vary between symbolic and substantive adopters.
H3: the relationship between EHR meaningful-use and the likelihood of data breaches will significantly vary between symbolic and substantive adapters.

Figure 2: Conceptual Model of Influence of EHR Meaningful-use and IT Security Investment on Likelihood of Data Breaches, Moderated by Symbolic/Substantive Adoption

Research Methodology

Data

This study will use several sources to construct a rich panel data set including the majority of U.S. hospitals from 2008 to 2015. By utilizing hospitals data collected from the Healthcare Information and Management Security Society (HIMSS) Analytics database, we have access to information about meaningful-use attestation, attestation date, and the adoption of health IT systems. This dataset also includes other variables such as financial outcomes and general descriptions of these hospitals which we use as control variables. We can obtain the majority of data on breaches in the healthcare industry by the breaches information from U.S. Health & Human Services (HHS) and the Privacy Rights Clearinghouse websites (www.hhs.gov & www.privacyrights.org). These websites provide a comprehensive list of publicly announced data breaches and have served as a single source of information in recent research (Sen & Borle, 2015).

Model Specification

Following the study by Angst et al. 2017, we use latent class models to find evidence for two classes of symbolic and substantive adopters. Further, to identify the changes in breach performance consequent to IT security investment and EHR meaningful-use, moderated by symbolic or substantive adoption, we use Fixed-effect panel approach and Propensity score matching (PSM). PSM is widely used to select treatment and comparison groups who resemble each other in all relevant characteristics before an event. This will allow us to create a statistical equivalence between the two groups (Rosenbaum & Rubin, 1983). Matching on a propensity score will enable us to identify a comparison group of hospitals with similar determinants of size, operating expenses, net income, the number of full-time employees, the number of beds, etc.

Contributions

This study aims to contribute to the institutional theory literature on health IT adoption by emphasizing the critical rule of the symbolic or substantive adoption under security failure risks. We improve and advance the notion of symbolic or substantive adoption by introducing characteristics such as coupling more complementary IT applications beyond the formal attestation of meaningful-use, such as financial systems, scheduling systems, and HR systems (for the future expansion we can also include clinical applications such as decision support systems applications). This improvement not only will be beneficial to explain the significant variation in the relationship between IT security investment (or meaningful-use) and the likelihood of data breaches among the hospitals; but also, such classification will be valuable for other areas of organizational research.
There is no doubt that security and privacy issues will be of central importance for patients, public healthcare systems and healthcare providers and organizations (Bishop et al., 2005). Thus, understanding the likelihood of data security breaches in hospitals would be valuable for the managerial audience in hospitals and healthcare providers in terms of the process of making future business strategies. Therefore, providing such information that enhances privacy, security, and confidentiality is critical to address the increasing cybersecurity threats and risks associated with them. Such knowledge can improve IT security literature and further shed light on strategic IT adoption (EHR) that enhances healthcare performance while addressing IT security effectiveness. Finally, the findings of the current research will be crucial for the policymakers in terms of the process of building the future legislation to improve the wellbeing of all EHR’s stakeholders. In doing so, we hope to increase the awareness of policy makers in targeting ample policy responses in other counties, specifically the United States.

REFERENCES


